AlphaGIGABIT Secure Wireless Router 8800

User Manual

Over 1.5 million square feet of coverage

with PowerZONE Technology



ALPHA SHIELD®
SECURE NETWORKING

Table of Contents

Table of Contents

Table of Contents

1. INTRODUCTION:

Congratulations on your purchase of the AlphaGIGABIT Secure Wireless Router 8800, and thank you for choosing AlphaShield for your networking and security needs. Your new router allows you to share files and printers on your network, and surf the Internet with the performance benefits of network optimization using StreamEngine® Technology, PowerZONE Technology, Gigabit Ethernet and Turbo Wireless-G and the built-in security benefits of the AlphaShield firewall with AlphaGAP® technology. Soon, you will be able to have a secure and enjoyable Internet experience.

Your AlphaGIGABIT Secure Wireless Router 8800 has been designed for maximum duty uptime. The only time it requires you to take it offline is briefly during setup and occasionally to upgrade the firmware program inside the router. As an added security measure, you can instantly isolate your computer(s) from the Internet at the press of a button.

This manual will show you how to set your new router, and to get your computer(s) connected to the Internet. Once you are online, we invite you to visit the AlphaShield website www.alphashield.com to register your new product, check for firmware updates and activate any subscription-based services that have been bundled with your router. At the website, you will also find additional tips and knowledge based articles to assist you with getting the most out of your networking experience.

2. CONTENTS:

1. AlphaGIGABIT Secure Wireless Router 8800
2. Cat5 Ethernet Cable
3. Power Adapter (6.8V, 2.5A)
4. Quick Installation Guide
5. CD-ROM with Manual
6. Vertical Stands

Note : Please contact your reseller if any of the above items are missing.

Important: Using a power supply other than that included with your router will result in the warranty of this product being declared void.

3. SYSTEM REQUIREMENTS:

1. External xDSL or Cable Modem with Ethernet Ports.
2. PC or MAC with following minimum requirements:
   - 1.25 Ghz processor
   - 256MB Memory
   - CD-ROM Drive
   - Ethernet Adapter 10/100/1000 with TCP/IP Protocol Installed
   - Windows® XP/2000/Vista/ME or Mac® OS X v10.3/v10.2/v10.1or Linux
   - Internet Explorer v6, Netscape® Navigator v7 or Firefox v1.5

4.FEATURES:

Hardware Interface Features:

Router/Switch Hardware:

- Dedicated 250 MIPS High Speed core Network Processor
- Dedicated High Speed Multi-port Gigabit Switch & Co-Processor
- 5 x 10/100/1000 Auto-Sensing Gigabit Ethernet LAN Ports with MDI /MDI-X
- 1 x 10/100 Auto-Sensing Fast Ethernet WAN Port with MDI/MDI-X
- 4 Universal Serial Bus (USB) connections
- Atheros Chipset & 802.11 b/g transceiver with Super G 108 Mbps wireless throughput

Router Features:

- WAN and LAN USB Network Storage
- USB Print Server Capability
- Static and Dynamic Network Address Translation (NAT)
- Secure LAN and WAN HTTP Router management
- Static and Dynamic DHCP WAN Mode
- Supports Virtual Server Access
- Built-in DHCP Server
- Dynamic DNS and Port Forwarding
- StreamEngine Technology® for Packet prioritization of Real-Time Applications
- Supports IPSec VPN (Virtual Private Network)
- Ethernet speed and link status LED indicators
- One Click Configuration Setup Wizard

Wireless Features:

- 802.11 b/g and Super G Wireless Connectivity
- Configurable and Extended Range settings of up to 1500 feet
- Supports WEP 64 and 128 bit encryption keys
- Provides WPA and WPA 2 - Personal and Enterprise Security
- High gain 7dBi omni-directional main antenna
- Dual Antenna Technology (DAT) with Polarization Diversity
- Supports Wireless Distribution System (WDS)
- Supports IEEE 802.11d Standard

AlphaShield Firewall:

- AlphaGAP Logical Disconnection and Re-connection
- Full Stateful Packet Inspection (SPI)
- AlphaGAP Scheduler
- IP-Stealth technology
- Configurable DMZ Option
- Inclusion, Exclusion MAC and IP filtering
- Parental Web Access Control
- User Selectable Logging support
- LAN, WAN and Wireless Network Traffic Statistics

Additional Features:

- Network Time Protocol
- WAN Mode: Static, DHCP, PPPoE, PPTP, L2TP and Bigpond
- Other Protocols Support: RIP, IGMP, and DNS Relay
- Application Level Gateway Configuration for: MSN, FTP, NetMeeting, IPSec VPN, MMS, SIP, Wake On LAN, PPTP
- Pre-selectable and Configurable Port Rules for Gaming
- Internal Online Help Guide
- 1.5 million square feet of coverage with PowerZone Technology.

Support:

- AlphaShield Limited Life-Time Warranty
- Automatic Firewall Upgrade Notification
- Free Online and Telephone Technical Support

5.HARDWARE GUIDELINES:

5.1 Connections:

1. All Ethernet Ports (WAN and LAN) are auto MDI/MDIX, meaning you can either use a straight-through or a crossover Ethernet cable.
2. 5 **Auto MDI/MDIX LAN ports** automatically sense the cable type when connecting to Ethernet-enabled computers for both WAN and LAN.
3. The **Auto MDI/MDIX WAN** port is the connection for the Ethernet cable to the Cable or DSL modem.
4. Pressing the **Reset Button** will restart the Router.
5. Pressing the **AlphaGAP Button** will disconnect your computer from the Internet.
6. Receptor for the **Power Adapter.**

5.2 LEDs:

5 LOCAL NETWORK LEDs:

The connection to an Ethernet-enabled computer on ports 1-5 is indicated by a solid light. When data is being transmitted, this LED will flash.

1 POWER LED:

A solid light indicates a proper connection to the power supply.

1 WAN LED:

A solid light indicates connection on the WAN port. When data is being transmitted, this LED will flash.

1 WLAN LED:

When there is activity on the wireless network, this LED will flash.

1 AlphaGAP LED:

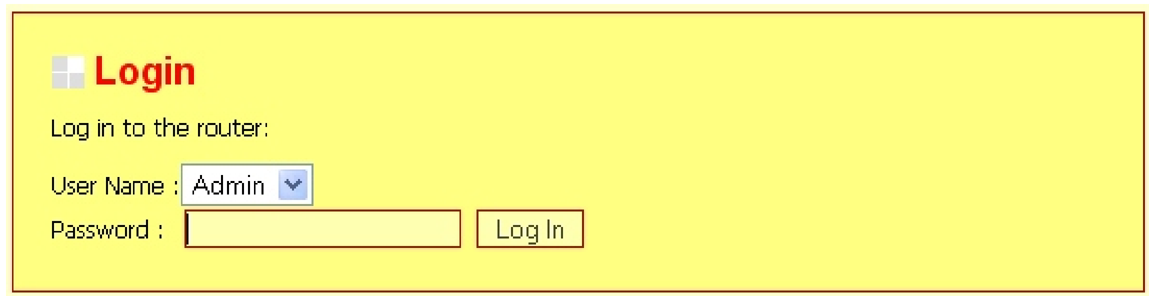
A Solid RED light will signify that the Router is in AlphaGAP Mode and Solid Green will signify that the Router is in Connected Mode.

6. LOGIN:

The Configuration Interface can be accessed from your Web browser. Type http://192.168.0.1 in the address window and press Enter.

The Login screen will appear.

- Select a **User Name**.
- By default, there is no password. Simply leave this window blank
- Click **Log In** to proceed.

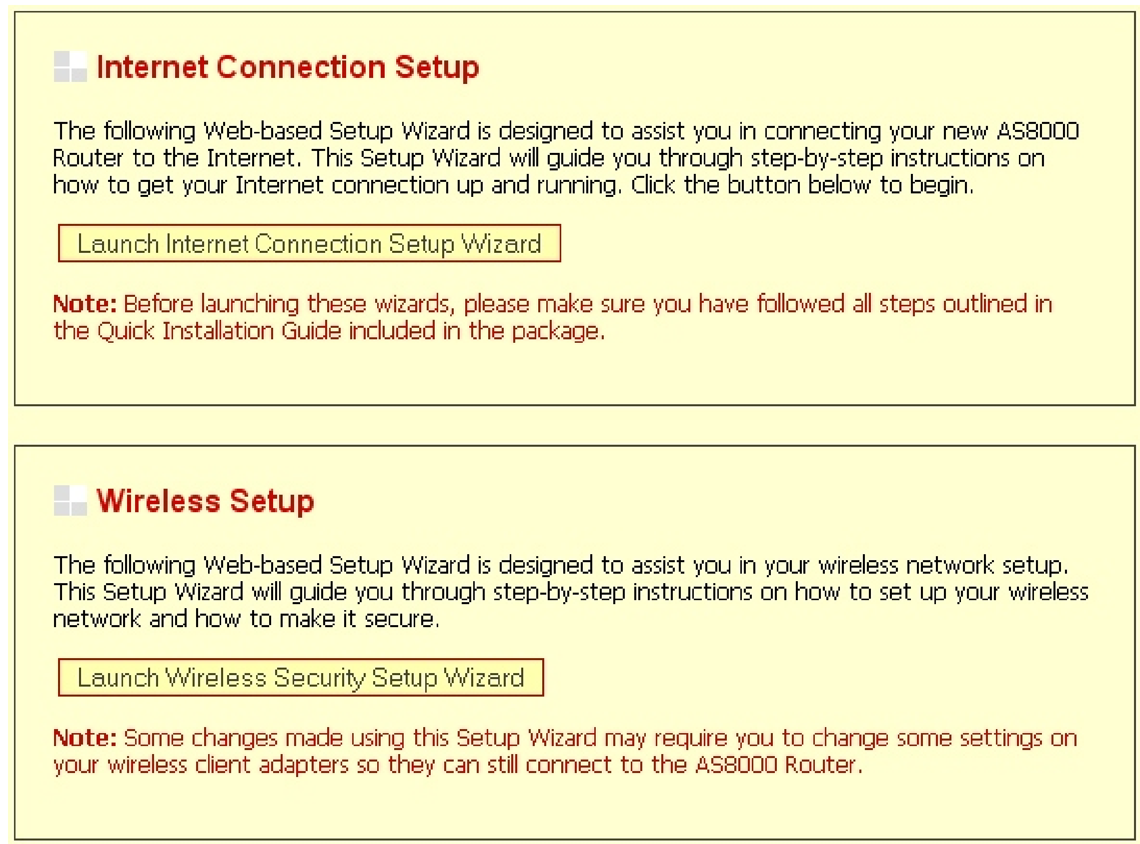


7. SETUP:

7.1 Quick Start:

The Wizard screen contains two wizards:

- **Internet Connection Setup**
- **Wireless Setup**



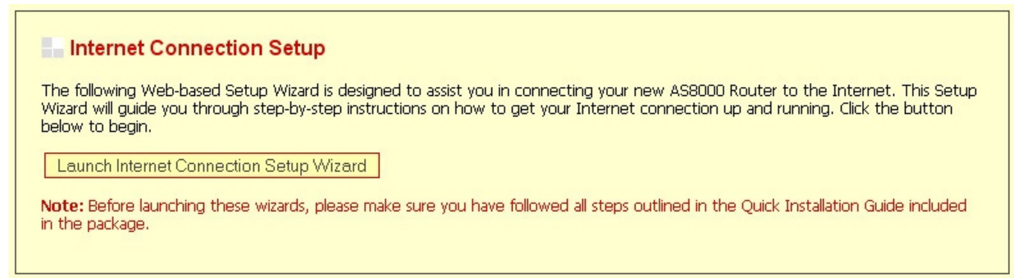
a) Launch Internet Connection Setup Wizard:

The following Web-based Setup Wizard will help you connect your new AlphaGIGABIT Router to the Internet. This Setup Wizard will guide you in a step-by-step manner to get your Internet connection up and running.

Before launching the Wizard, please make sure you have correctly followed all of the steps outlined in the Quick Installation Guide included in the package.

SETTING UP THE ROUTER:

- ✍ Click the **Launch Internet Connection Setup Wizard**.



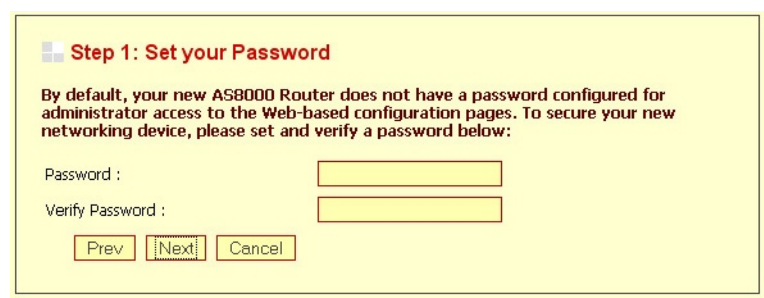
Now you will see **Welcome To The AlphaShield Setup Wizard** screen.

- ✍ To continue click **Next**



Step 1: Set your Password

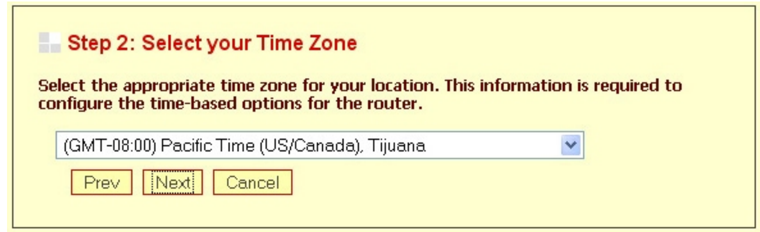
- ✍ Enter a Password of your choice
- ✍ To **Verify your Password,** re-enter it below
- ✍ To continue click **Next**



Step 2: Select Your Time Zone

Select your local time zone from the pull-down menu.

✍ To continue click **Next**



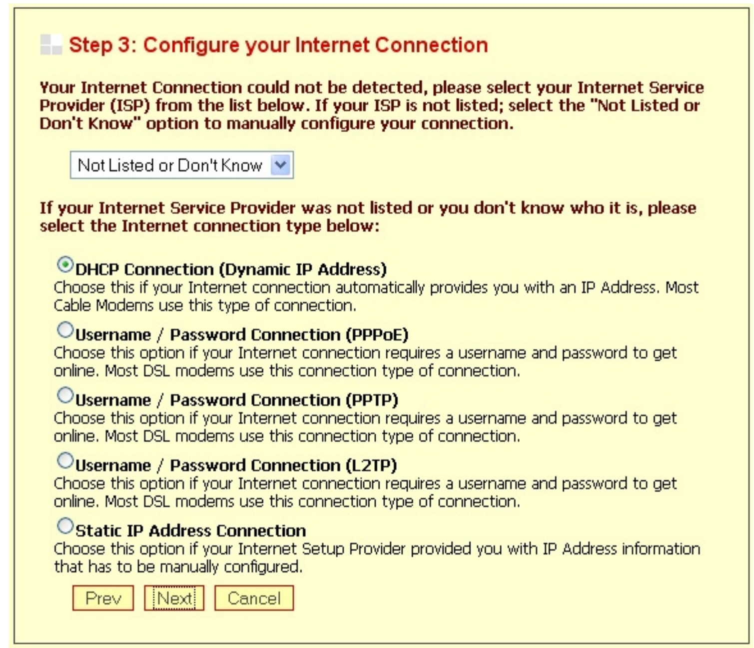
Step 3: Configure Your Internet Connection

From the pulldown menu, choose your Internet Service Provider (ISP).

If your ISP is not listed in the menu, or you do not know who your ISP is, simply select **Not Listed or Don't Know** from the menu.

If you require details, please contact your Internet Service Provider. If you selected **Not Listed or Don't Know** from the menu, choose one of the five connection options which best applies to your Internet service.

✍ To continue click **Next**



Step 3: Configure Your Internet Connection

DHCP CONNECTION (Dynamic IP Address)

A **MAC Address** is a unique hardware address for devices on a Local Area Network.

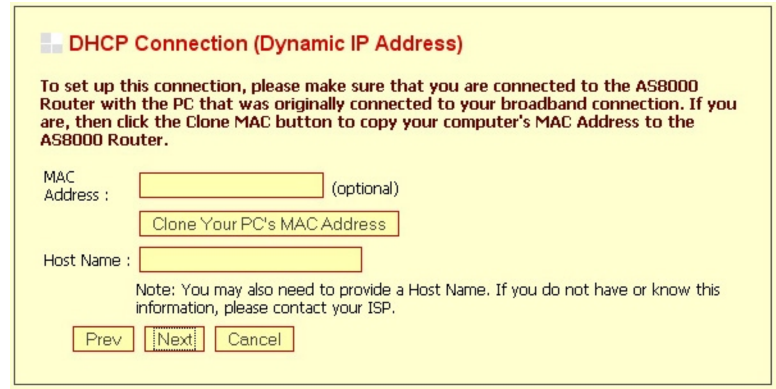
Enter the **MAC Address** of the computer that was originally connected to your broadband modem.

If the computer you are using was the initial system connected to your broadband modem, simply select Clone your PC's MAC

Address and the MAC Address will automatically appear.

✍ Enter a **Host Name** (If your ISP requires one).

✍ To continue click **Next**



Step 3: Configure Your Internet Connection

Set Username and Password Connection (PPPoE)

✍ Enter **your Username**

✍ Enter your Password

✍ To verify your Password, re-enter it below

✍ Enter a **Service Name** (if your ISP requires one)

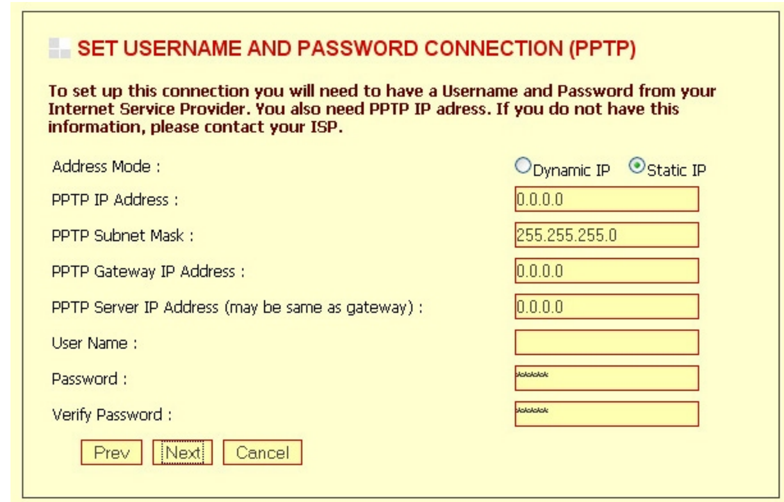
✍ To continue click **Next**



Step 3: Configure Your Internet Connection

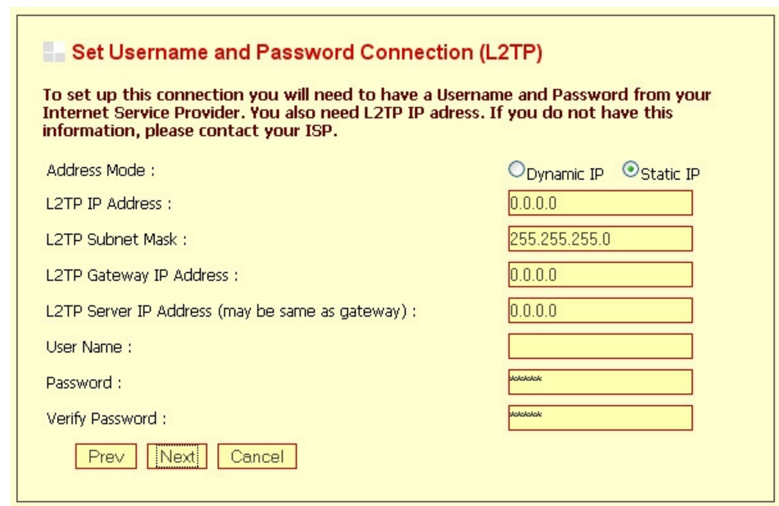
At the Set Username and Password Connection (PPTP) Enter:

- **PPTP IP Address**
- **PPTP Subnet Mask**
- **PPTP Gateway IP Address**
- **PPTP Server IP Address**
- **Your Username**
- **Your Password**.
- To verify your **Password**, Re-enter it below
- To continue click **Next**



At the **Set Username and Password Connection (L2TP)** screen enter:

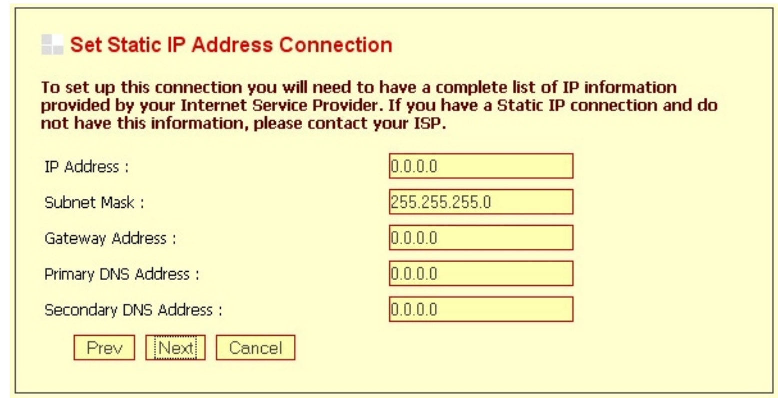
- **L2TP IP Address**
- **L2TP Subnet Mask**
- **L2TP Gateway IP Address**
- L2TP Server IP Address
- Your Username
- **Your Password**.
- To verify your **Password**, re-enter it below
- To continue click **Next**



At the Set Static IP Address Connection

Enter:

- **IP address**
- **Subnet Mask**
- **Gateway Address**
- **Primary** and **Secondary DNS Addresses**
- To continue click **Next**



Setup Complete

- Click **Connect**. This will save your settings and reboot the router



b) Launch Wireless Security Setup Wizard:

The next step is to set up your wireless network. This Wizard will help you set it up and make it secure. Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the AlphaGIGABIT Route:

Wireless Setup:

- Click **Launch Wireless Security Setup Wizard** to begin.



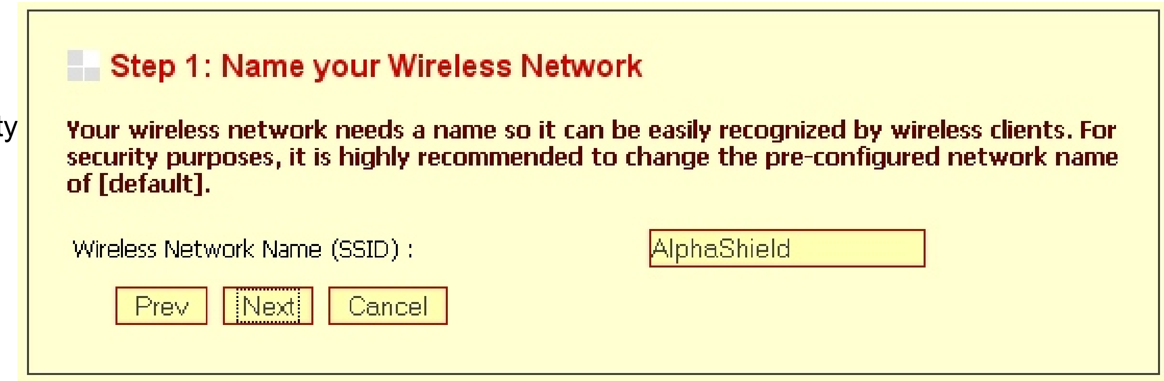
Welcome To The AlphaGIGABIT Wireless Security Setup Wizard:

- Click **Next** to continue.



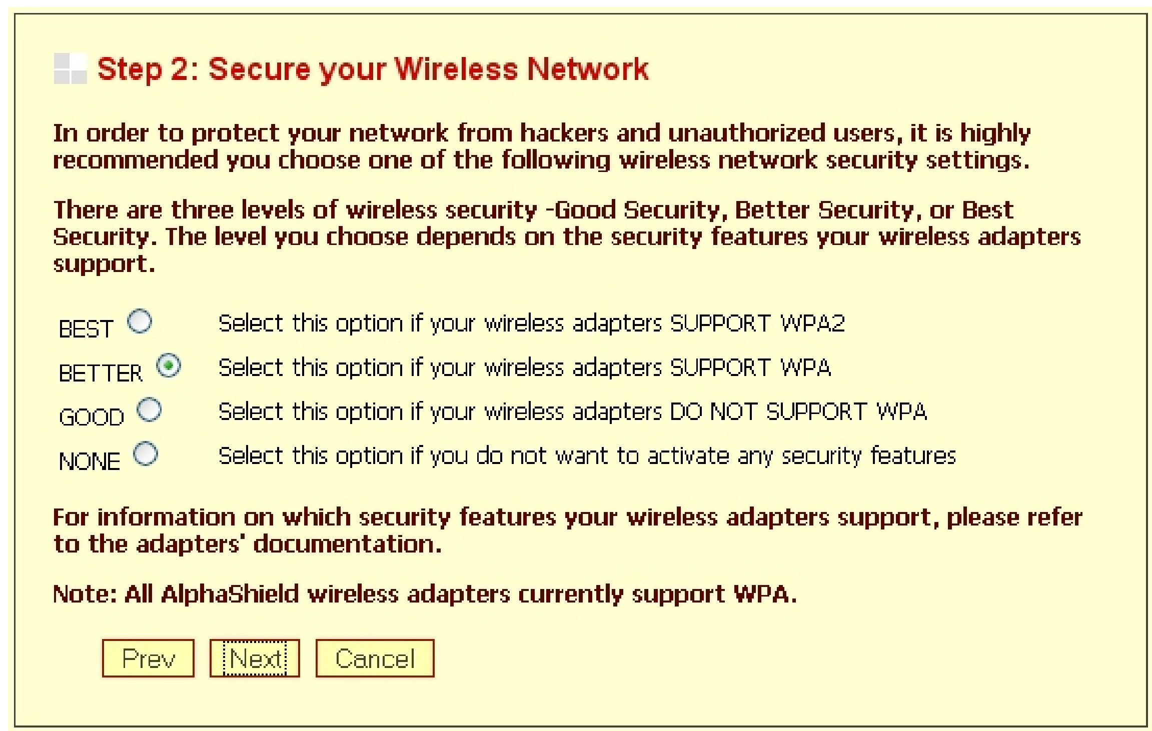
Step 1: Name Your Wireless Network

- Choose a Name for your Wireless Network
- Do not choose the default name for security reasons
- To continue click **Next**.



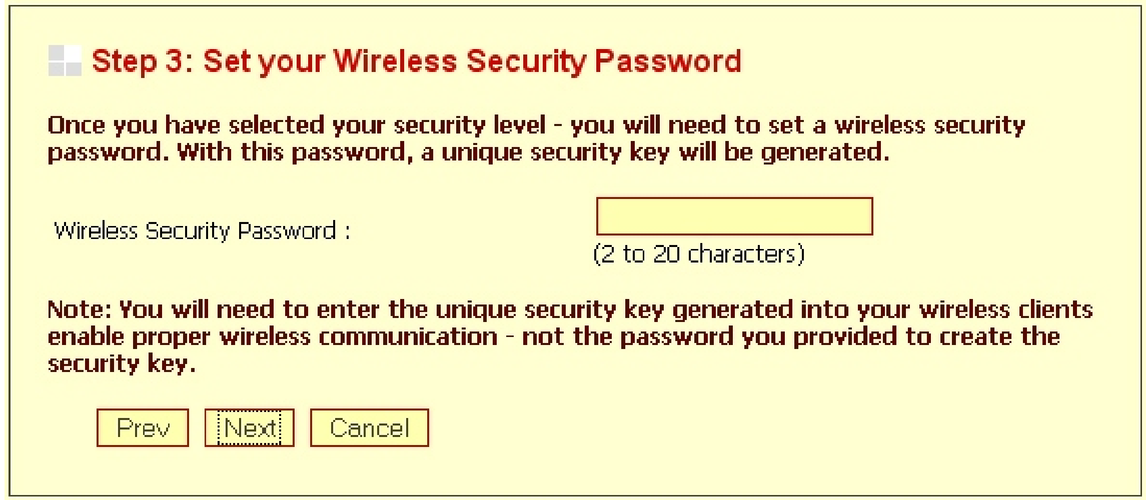
Step 2: Secure Your Wireless Network

- Choose a security option to protect your network from unauthorized users.
- To continue click **Next**



Step 3: Set you Wireless Security Password

- Select a Security Password between 2 and 20 characters
- To continue click **Next**

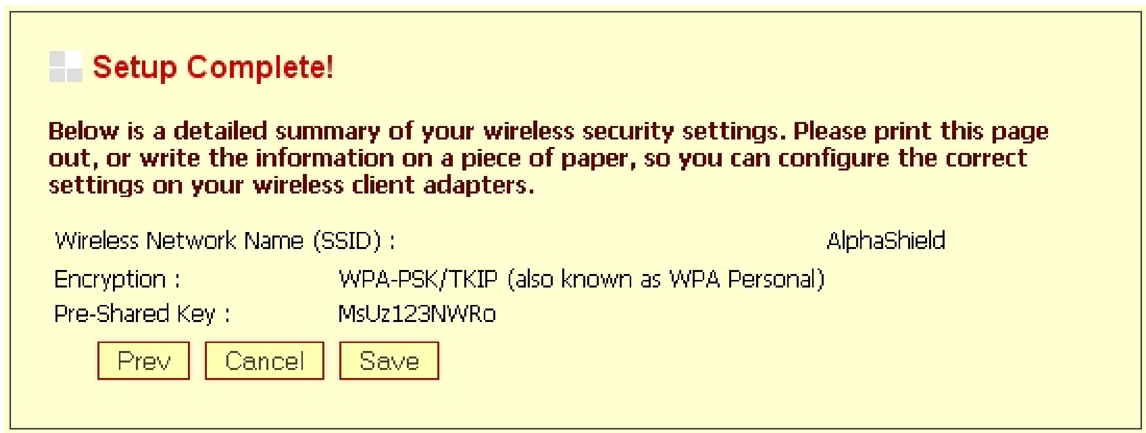


Setup Complete!

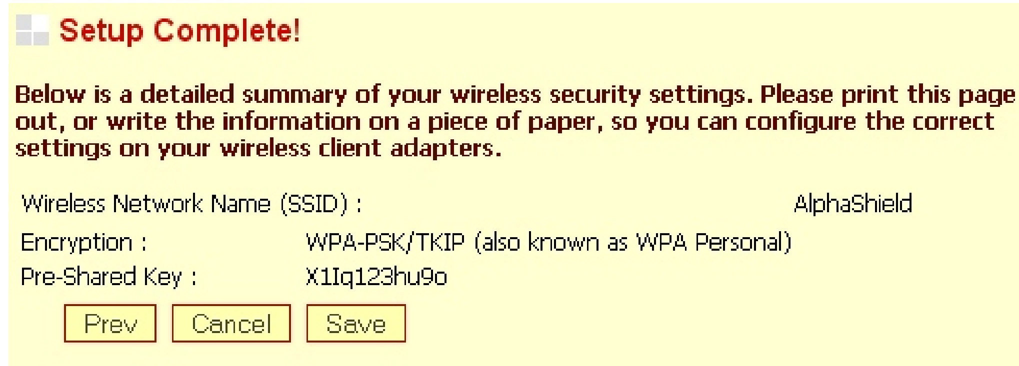
The setup Page will give you a detailed summary of the settings, based on what you have selected in the previous steps.

- Click **Save** to continue

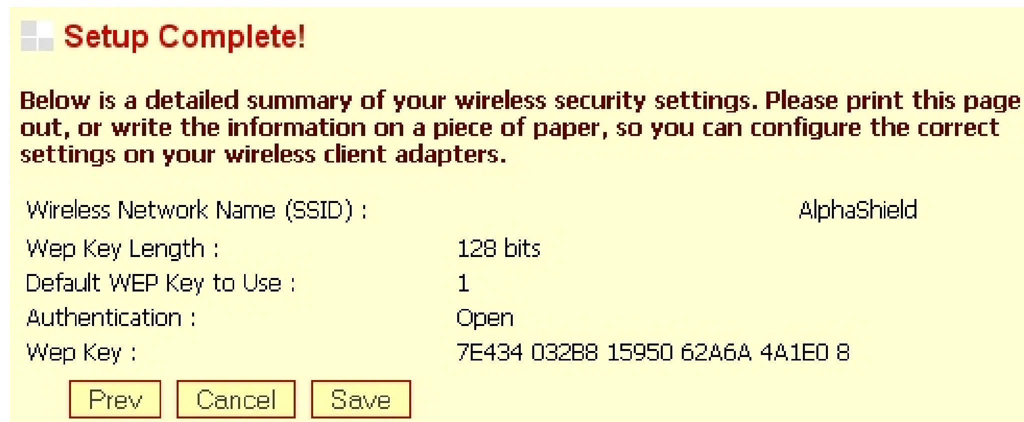
This screen will only appear if you selected BEST security



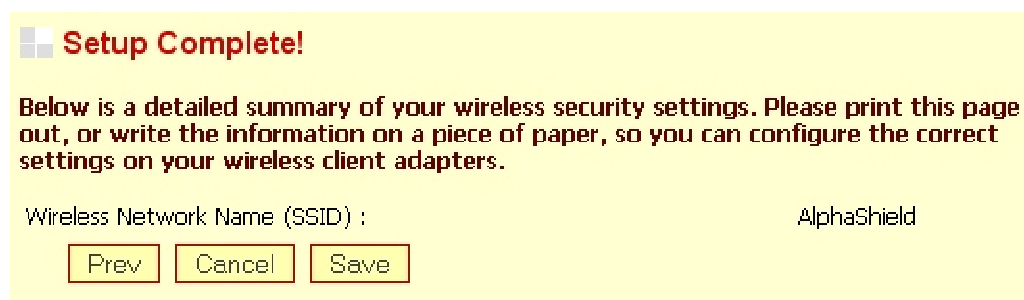
This screen will only appear if you selected BETTER security



This screen will only appear if you selected GOOD security



This screen will only appear if you selected NONE security

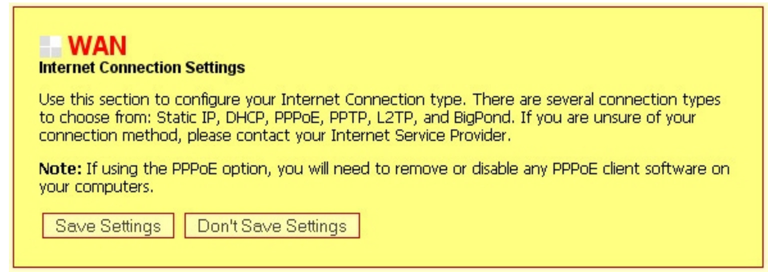


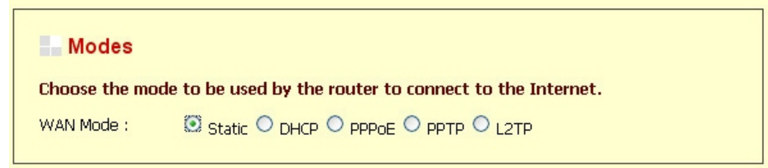
7.2 WAN:

The WAN section will help you choose one of 6 connection types: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers. If you have any questions about your connection, please contact your Internet Service Provider (ISP).

a) Modes:

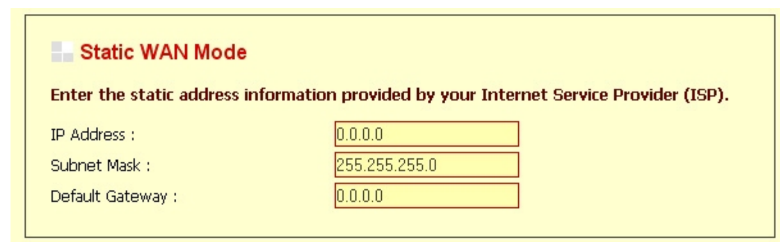
- Choose one of 6 modes of connection for the router.
- If you are unsure of your connection settings, contact your Internet Service Provider (ISP).

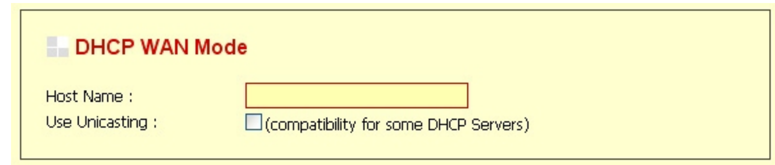




Static WAN Mode:

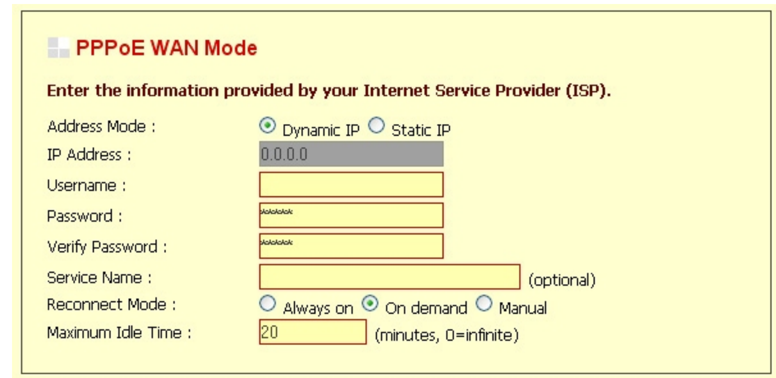
- Enter the **IP Address** from your router configuration settings provided by your ISP or network administrator.
- Enter the **Subnet Mask** from your router configuration settings provided by your ISP or network administrator.
- Enter the **Default Gateway** address from your router configuration settings provided by your ISP or network administrator.





DHCP WAN Mode:

- Enter a **Host Name** to identify your system to the ISP's server



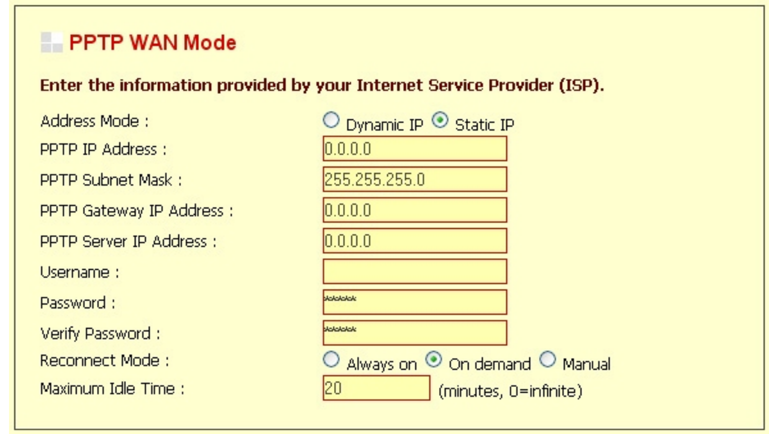
PPPoE WAN Mode:

- **Enter the Username** and **Password** you use to gain access to the Internet.
- To verify your **Password**, re-enter it below
- Enter a **Service Name** (If your ISP requires it).

Reconnect Mode

- **Always on**: The Internet connection is always maintained.
- **On Demand**: The Internet connection is made when the user chooses to log on.
- **Manual**: The user must push the button **Manually** to connect to the Internet.

(PPPoE WAN connections are not necessarily always online).



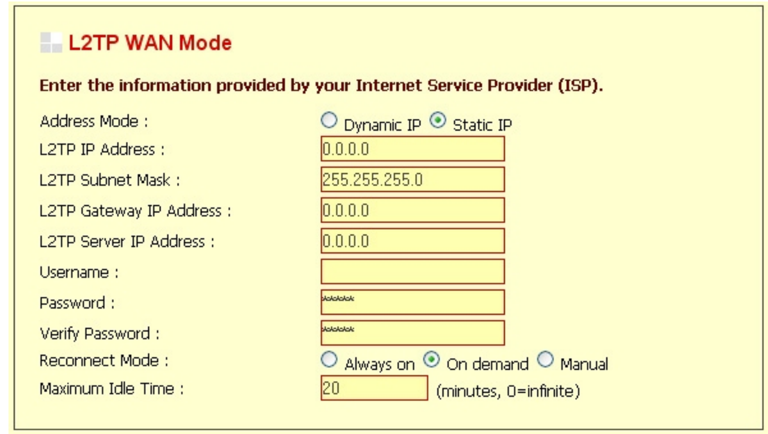
PPTP WAN Mode:

- Enter the **PPTP IP Address** provided by your ISP.
- Enter the **PPTP Subnet Mask** provided by your ISP.
- Enter the **PPTP Gateway IP Address** provided by your ISP.
- Enter the **PPTP Server IP Address** you are connecting to, also provided by your ISP.
- **Enter the Username** and **Password** you use to gain access to the Internet.
- To verify your **Password**, re-enter it below.
- Select the **Maximum Idle Time** before the PPTP connection is disconnected.

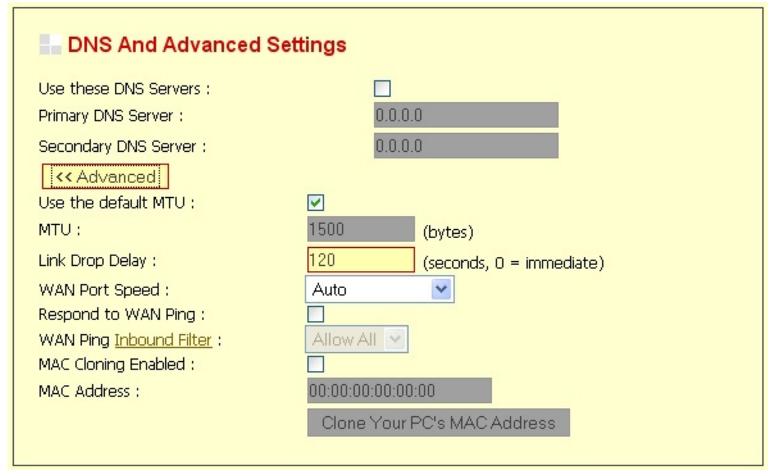
L2TP WAN Mode:

Enter:

- The **L2TP IP Address** provided by your ISP.
- The **L2TP Subnet Mask** provided by your ISP.
- The **L2TP Gateway IP Address** provided by your ISP.
- The **L2TP Server IP Address** provided by your ISP.
- **Enter the Username** and **Password** you use to gain access to the Internet.
- To verify your **Password**, re-enter it below.
- Select the **Maximum Idle Time** before the L2TP connection is disconnected.



DNS And Advanced Settings:

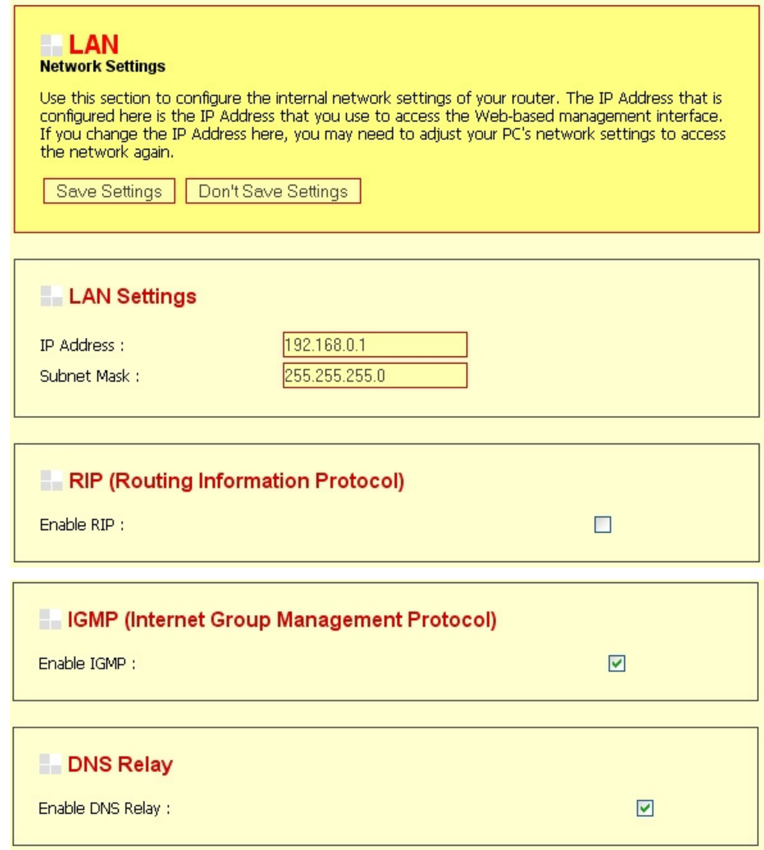


These Options may be used on all WAN Modes:

- If you have the DNS servers provided to you by the ISP, please select the **Use these DNS Servers**
- Please enter the **Primary DNS Server** provided by your ISP
- Please enter the **Secondary DNS Server** provided by your ISP
- **Use the Default MTU** is enabled by default
- **MTU**(Maximum Transmission Unit) determines The largest packet size (in bytes) that the router will send to the WAN. The MTU must be set to match the MTU settings of your ISP connection. If the router's MTU is set too high or low network performance can suffer. For an Ethernet connection, values are 1500 bytes and 1492 bytes for a PPPoE connection. The Router will use the default value assigned in the **MTU** window.
- **WAN Port Speed** is set to Auto by default. You can select the connection type (10 or 100Mbps) if you have trouble connecting the WAN port.
- **Respond to WAN Ping** is disabled by default. The Router will not respond to requests from a ping command received via the Internet. Hackers commonly Use WAN Ping IP addresses to test whether your WAN IP address is valid.
- **MAC Cloning Enabled.** When this box is checked, The **MAC address** does not need to be entered manually in the next window. The WAN port will use the MAC Address of the network adapter in the computer that you are using to access the router.

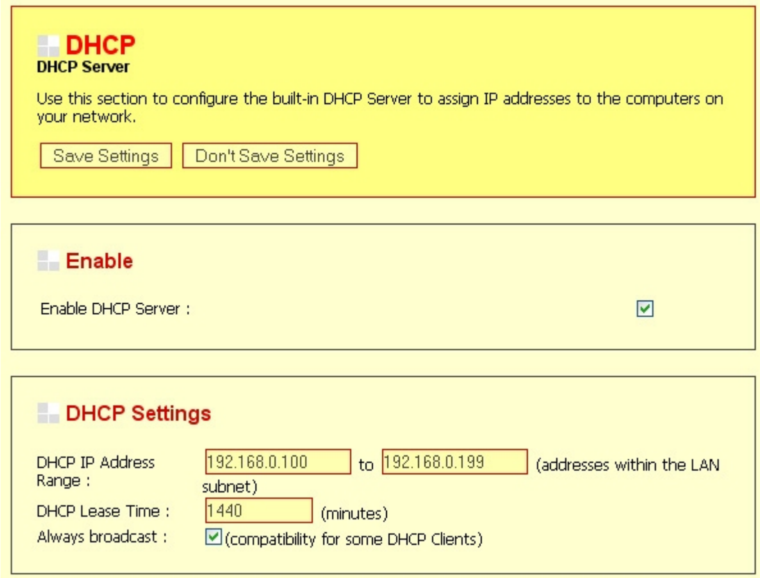
7.3 LAN Settings:

- **IP Address:** Enter the IP address of the router on the local area network. The local network settings are based on the address assigned here.
- **Subnet Mask:** Use the of your router on the local area network.
- **RIP Announcement is u**sed with multiple routers to broadcast routing information.
- **Gateway Metric** is only used if you have multiple routers.



7.4 DHCP:

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.



DHCP Settings:

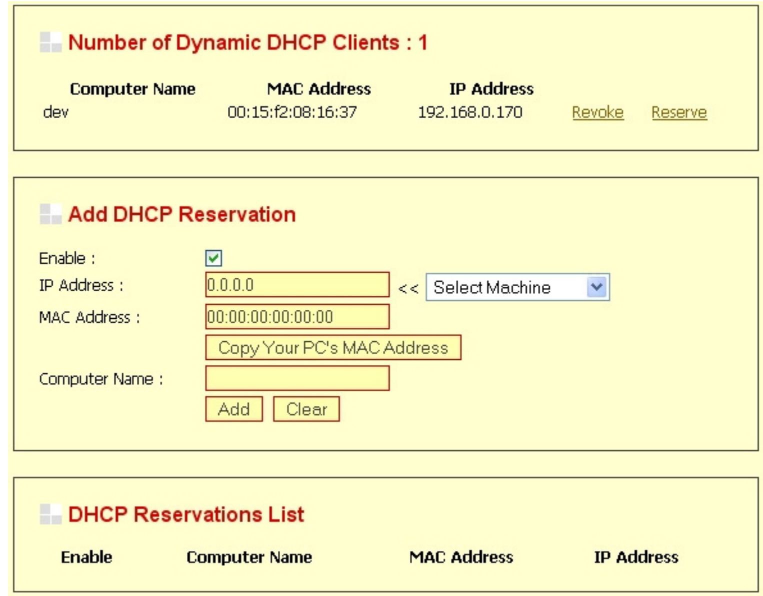
To connect to the LAN and Internet the DHCP Server function will assign your network devices the necessary information and you do not have to manually configure each device on your network with IP settings. The devices on your network must have TCP/IP bound to the Ethernet connection with the "DHCP" or "Obtain an IP address automatically" option enabled.

✍ **DHCP IP Address Range** defines the range of addresses available for the Router to assign to your internal network.

Note: If you have any devices using static IP addresses, be sure the addresses do not fall within the range defined in the **DHCP IP Address Range** field. A Static IP address is one that is entered in manually on the device.

✍ **DHCP Lease Time** determines the amount of time a computer may have an IP address before it is required to renew the lease. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease expires then a new lease is established. If the lease expires and the address is no longer needed, and then another tenant may use the address.

Number of Dynamic DHCP Clients:



- This is used to automatically assign IP addresses from a predetermined pool of addresses to computers or devices that request them. It shows the number of clients that are receiving an IP address from the router and LAN devices those are leasing IP addresses.
- The **Computer Name, MAC Address**, and **IP Address** assigned to each computer are displayed here as well. With the **Revoke** option you can cancel a leased IP address. This feature is useful for freeing up addresses when the client table is full or nearly full.

Add DHCP Reservation:

MAC address:

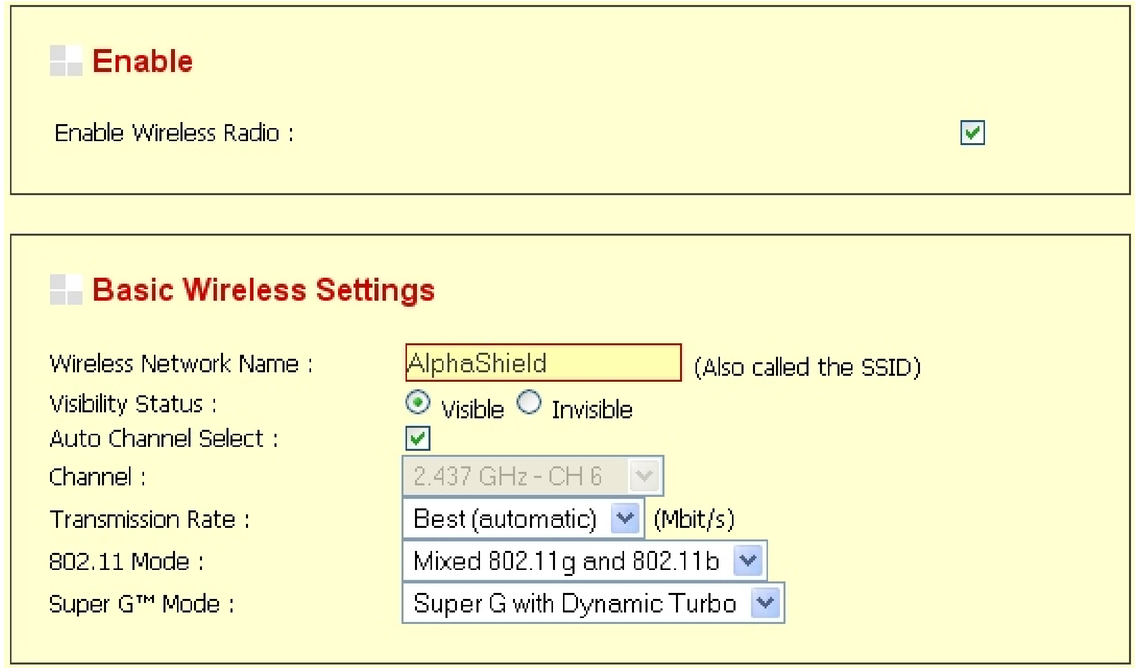
- Enter the **MAC address** manually or connect to the AlphaShield Router's Web-Management interface from the system and click **Copy Your PC's MAC Address**.

Note: If you replace the Ethernet adapter in a computer that is using Static DHCP, you will need to Copy the PC's MAC Address again because every Ethernet adapter has a unique MAC address. The same goes for any network device. If you replace a network device such as a print server, you will need to input the MAC address of the new print server into the Static DHCP configuration. If your network device is a computer and the network card is already located inside the computer, you can use the **Copy Your PC's MAC Address** option to enter the **MAC address**.

DHCP Reservations List:

- **Enable** checkbox.
- When checked, the **DHCP Reservation List** can be enabled or disabled. To edit the entries click on the pencil icon. To delete the entries click on the trash can icon. If you have made some changes or deletions click **Save Settings** button at the top of the page.
- If your configuration settings are complete then click **Reboot the Device** otherwise click **Continue**. Your router must reboot before new settings will take effect.

7.5 Wireless:



Use this section to configure your wireless settings .

Your AlphaGIGABIT Router supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard; WPA provides a higher level of security; and WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Basic Wireless Settings:

- **Enable Wireless Radio**
  Check to enable this option
- **Wireless Network Name** also referred, as the SSID will appear in the list when you are browsing for available wireless networks.
- **Visibility Status allows you to** choose to make your wireless network to be Visible or Invisible. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal.

  If you're not using encryption then they could connect to your network. When invisible mode is enabled, you must enter the Wireless Network Name (SSID) manually to connect to the network.
- **Auto Channel Select** allows the router to automatically choose the best channel.
- **Channel** from the drop-down list with select the one with the clearest signal.
- **Transmission Rate** By default the fastest rate will be automatically selected. You can select the speed from the drop-down list.

Note: If all of your devices can connect in **802.11g Mode** then leave the setting at 802.11g only. If you have some devices that are 802.11b/g then you can change the mode to Mixed.

- **Super G Mode :** Super G Turbo Modes must use channel 6 for transmission and 802.11 Mode must be set to 802.11g.
- **Super G without Turbo:** Performance enhancing features such as Packet Bursting, Fast Frames, and Compression.
- **Super G with Static Turbo:** Mode is not backwards compatible with non-Turbo (legacy) devices. Static turbo enabled mode is always on and is only enabled when all devices on the wireless network are Super G with Static Turbo enabled.
- **Super G with Dynamic Turbo:** Mode is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are Super G with Dynamic Turbo.

Wireless Security Mode:

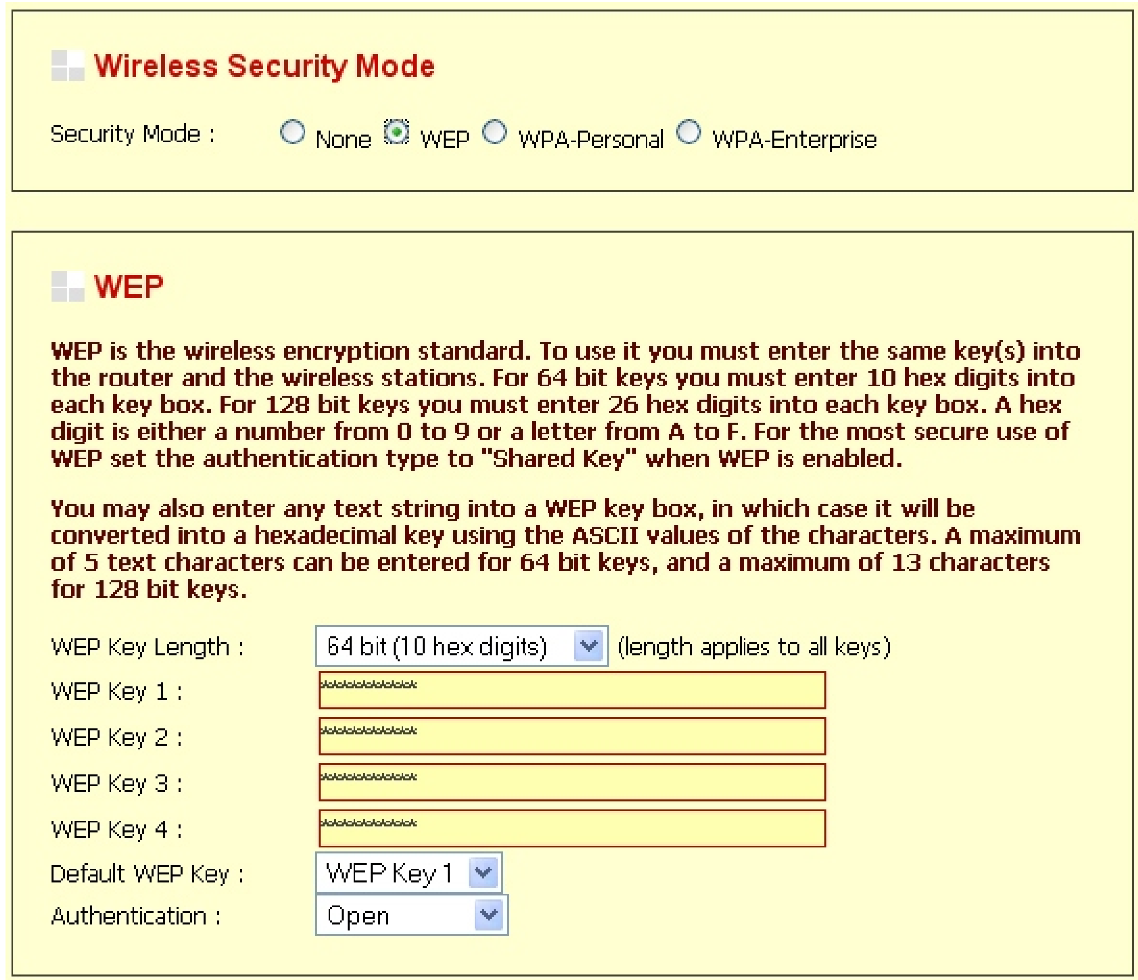
Configure the wireless security features to protect your privacy. Your AlphaShield Router supports three wireless security features; WEP, WPA-Personal and WPA-Enterprise wireless security modes.

The WPA-Enterprise option does require a RADIUS authentication server.

WEP

- WEP is the Wireless Encryption Standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

- You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

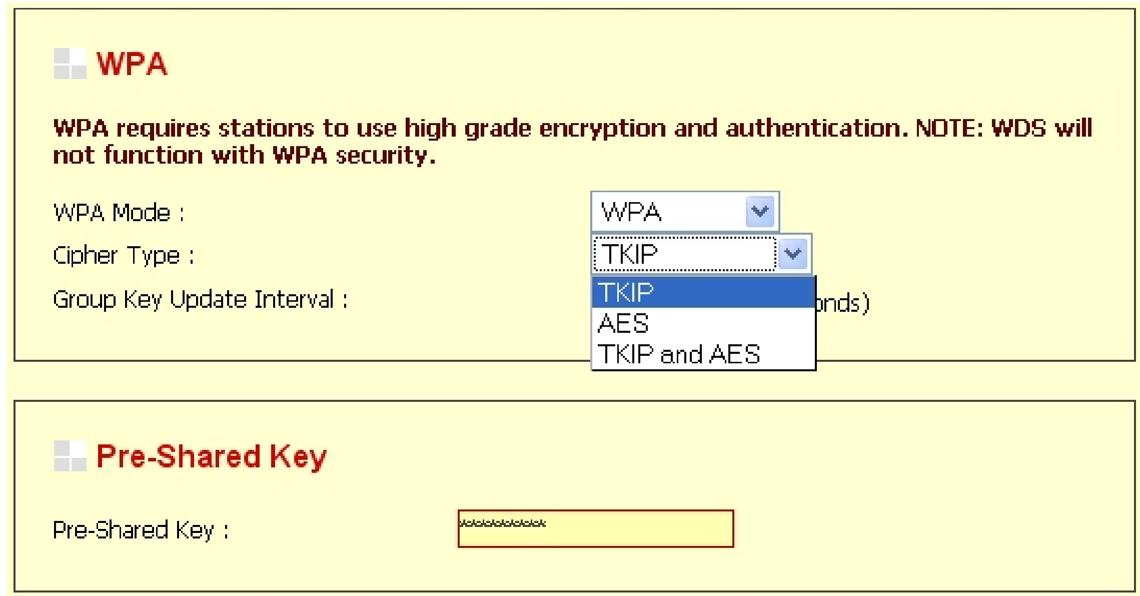


WPA-Personal:

- WPA requires stations to use high-grade encryption and authentication. WDS will not function with WPA security.

Select the **WPA Mode** from drop-down list:

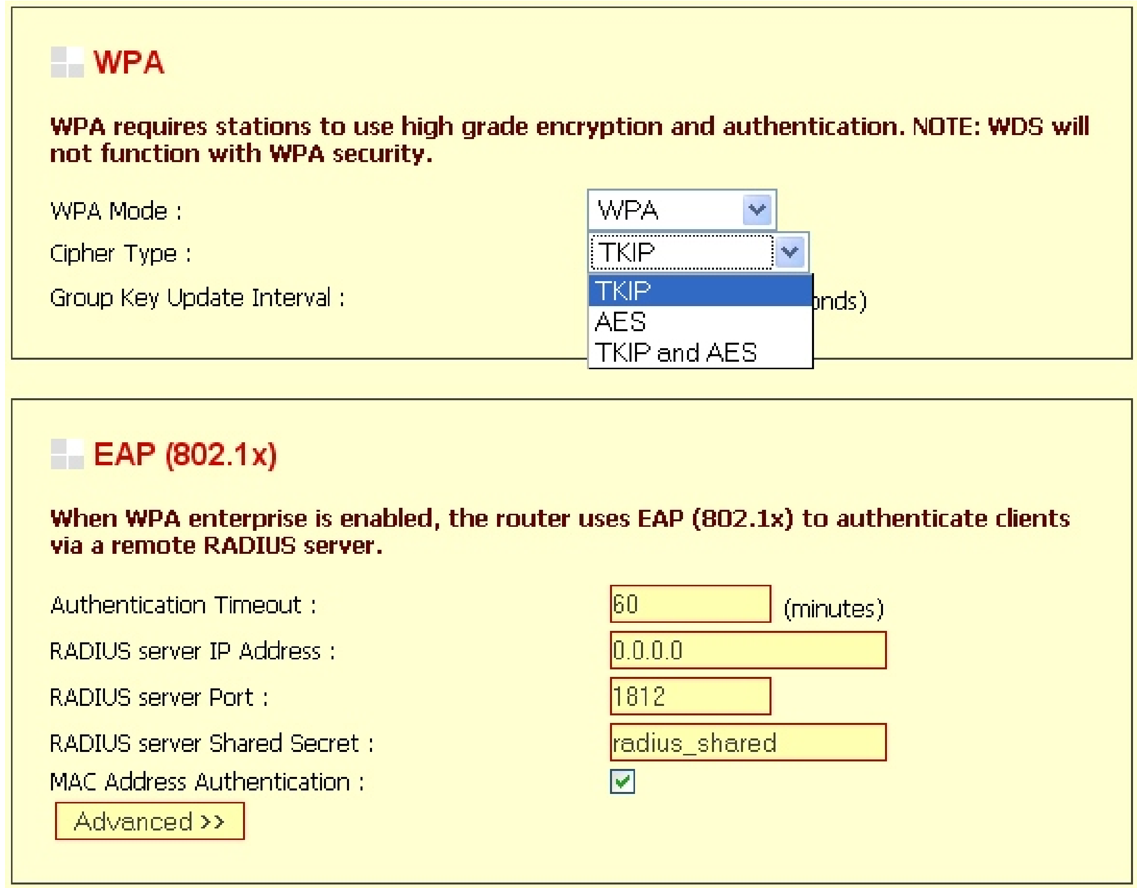
- **Cipher Type** is entered as a pass-phrase and used to generate session keys that are unique for each wireless client. It cannot be less than 8 characters and no more than 63 characters in ASCII format at both ends of the wireless connection. The pass-phrase cannot be shorter than 8 characters.
- **Group Key Update Interval** secures the data communication. TKIP (Temporal Key Integrity Protocol) provides per packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption.
- The amount of time before the group key used for broadcast and multicast data is changed.
- **Pre-Shared Key** uses Wi-Fi Protected Access.



WPA-Enterprise:

The RADIUS server works with WPA-Enterprise to authenticate wireless clients. The Server may need to be configured in order to do so. The necessary credentials should have been established by wireless clients before attempting to authenticate to the Server through the Gateway

- Select the pre-shared key **Cipher Type**.
- **Group Key Update Interval: Enter the Amount of** time before the group key used for broadcast and multicast data is changed.
- **Authentication Timeout:** Enter the time before a client is required to re-authenticate.
- Enter **RADIUS Server IP Address** i.e. address of the authentication server.
- Enter **RADIUS Server Port** the port number used to connect to the authentication server.
- Enter **RADIUS Server Shared Secret** is a pass phrase that must match with the authentication server.
- If **MAC Address Authentication** is selected then the user will need to connect from the same computer whenever logging into the wireless network.



8. ADVANCED:

Advanced Options allows you to configure a number of advanced features including ports, application priority, Internet access, filters, and advanced wireless settings.

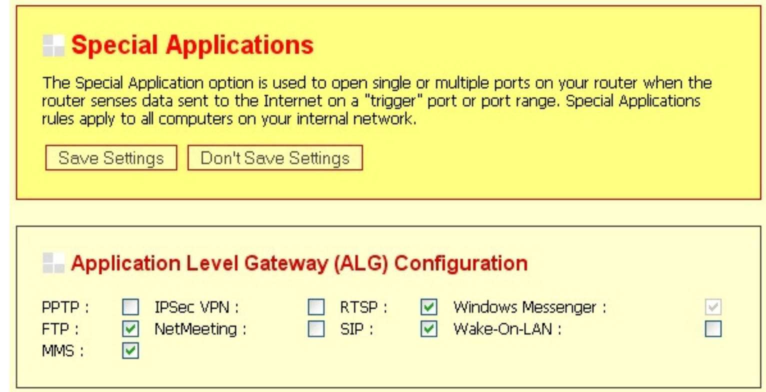
8.1 Virtual Server:

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.



- **Name:** Select a Virtual Server Rule (ex. Web Server) or select it from the drop down menu.
- **IP Address:** Enter the **IP Address** of the machine on your LAN 192.168.0.50 or you can select it from the dropdown menu.
- **Protocol**: Select the Protocol used by the service.
- **Private Port**: Enter the port that will be used on your internal network.
- **Public Port:** Enter the port that will be accessed from the Internet.
- **Schedule:** Select a time for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.
- **Save Settings:** click to save this information and continue

8.2 Special Applications:

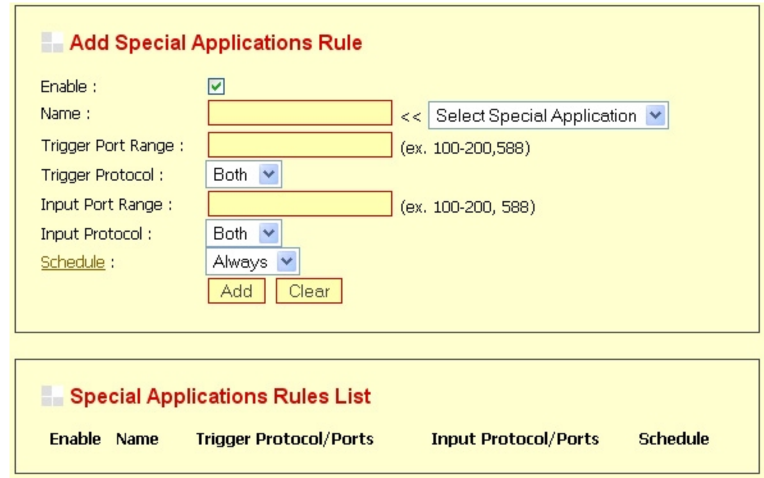


The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a 'trigger' port or port range. Special Applications rules apply to all computers on your internal network.

Application Level Gateway (ALG) Configurations:

Application Level Gateway (ALG) Configurations, also **known as ALG's** provide special handling for a specific protocol or application. By default, maximum ALG's for common applications are enabled, but this will allow you to enable or disable ALG's.

- **PPTP:** To check this box to allow multiple machines on the LAN and to connect to the corporate network.
- **IPSec VPN:** multiple VPN clients can connect to their corporate network. Some VPN clients support traversal of IPSec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off.
- **RTSP: When enabled, this allows** applications that use Real Time Streaming Protocol (RTSP) to receive streaming media from the Internet.
- **FTP: When this is enabled,** FTP clients and servers are allowed to transfer data across NAT.
- **NetMeeting: When enabled,** it allows Microsoft® NetMeeting clients to communicate across NAT
- **SIP:** This allows devices and applications using VoIP (Voice over IP) to communicate across NAT.
- **MMS:** Microsoft Media Services (MMS) allows Windows Media® Player, using MMS protocol, to receive streaming media from the Internet.
- **L2TP:** This allows multiple machines on the LAN to connect to their corporate network using the L2TP protocol.
- **Windows Messenger®:** This configuration allows all of the Windows Messenger® functions to work properly through the router.



Add/Edit Special Applications Rule:

The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications Rules apply to all computers on your internal network.

- **Rule Name:** Enter to identify the Special Application Rule in the future. You can also select from a list of common applications, and the remaining configuration values will be filled in accordingly.
- Enter the outgoing **Trigger Port Range** used by your application.
- Select the outbound **Trigger Port Protocol** used by your application.
- Enter the **Input Port Range** that you want to open up to Internet traffic.
- Select the **Input Port Protocol** used by the Internet traffic coming back into the router through the opened port range.
- Select a **Schedule** for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.
- **Save Settings:** click to save this information and continue.

Special Applications Rules List:

By toggling the **Enable** checkbox, the Special Application Rule List can be enabled or disabled. To edit the entries, click on the pencil icon. To delete the entries click on the trash can icon. If you have made some changes or deletions click **Save Settings** at the top of the page. If your configuration settings are complete, click **Reboot the Device**. Otherwise click **Continue**. The router must reboot before new settings will take effect.

8.3 Gaming:

The Gaming option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-50), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).



Add/Edit Game Rule:

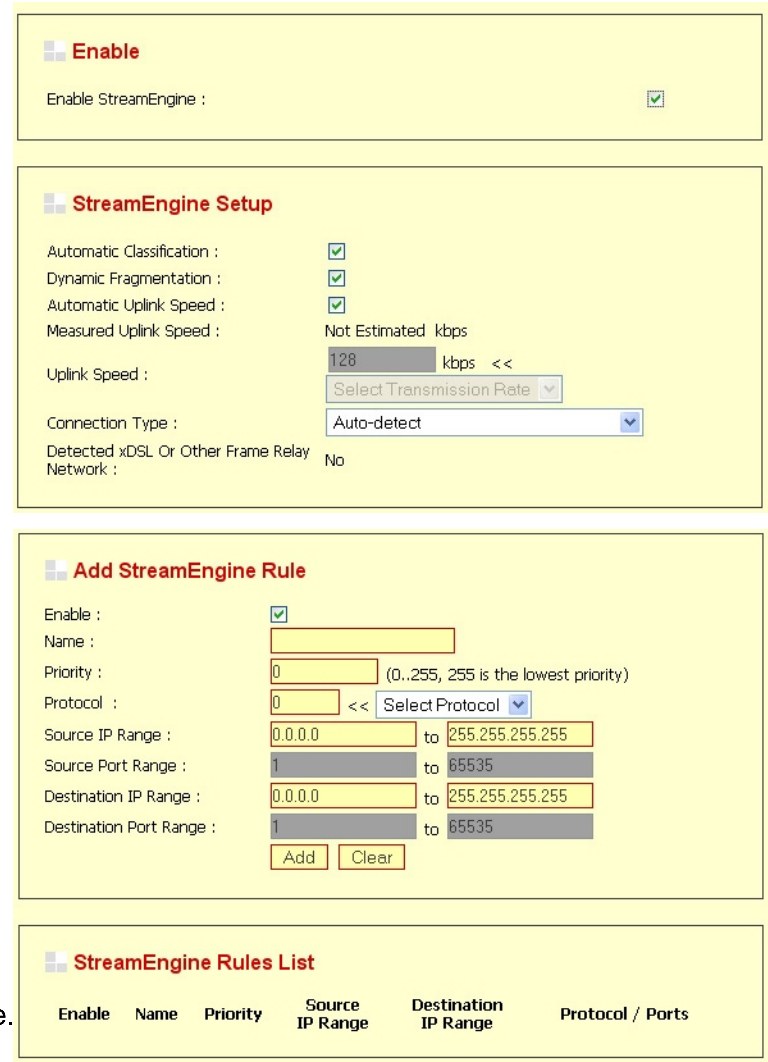
- **Rule Name:** Choose a Rule name that is meaningful to you or select from a list of pre-defined rules for many popular games. If you have any trouble with pre-defined rules, verify whether the port values have changed since the list was created.
- **IP Address**: Enter the local network IP Address of the system hosting the game server.
- Enter the **TCP Ports to Open.**
- Enter the **UDP Ports to Open.**
- Select a **Schedule** for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.
- **Save Settings:** click to save this information and continue.

Game Rules List:

Toggling the **Enable** checkbox enables or disables the Game Rule List. To edit the entries clickon the pencil icon. To delete the entries click on trash can icon. If you have made some changes or deletions click on **Save Settings** button on top of page. If your configuration settings are over then click the Reboot the Device button otherwise click Continue. The router must reboot before new settings will take effect.

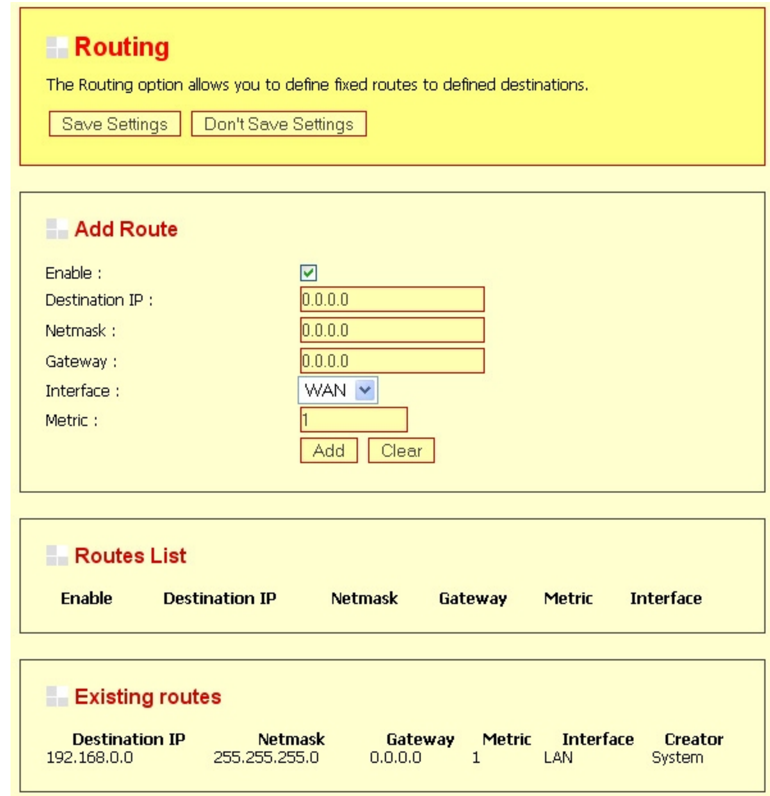
8.4 StreamEngine® Network Optimization:

This next section will help you configure the StreamEngine® Network Optimization. StreamEngine® Technology improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.



StreamEngine® Setup:

- **Enable StreamEngine®** is disabled by default. For better performance and experience for gaming, enable this Option.
- **Automatic Classification** will be enabled by default, when StreamEngine® is selected. This option will allow your router to automatically determine which programs should have network priority.
- When you have a slot Internet uplink, **Dynamic Fragmentation should** be enabled. It helps to reduce the impact that large low priority network packets can have more urgent ones on.
- **Automatic Uplink Speed:** This option will allow your router to automatically determine the uplink speed of your Internet connection.
- **Measured Uplink Speed** displays the detected uplink speed.
- **Uplink Speed** is the speed at which data can be transferred from the router to your ISP. Your ISP determines it.
- **Connection Type:** If you have an unusual network connection in which you are actually connected via DSL, but for which you configure either "Static" or "DHCP" in the WAN settings, changing the **Connection Type** to DSL or **Other Frame Relay Network** ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance.
- When Connection Type is set to automatic; the automatically detected connection type is displayed at **Detected XDSL or other Frame Relay Network**.



8.5 Routing:

Add/Edit Route:

The Routing option allows you to define fixed routes to defined destinations:

- **Destination IP:** Enter the Destination IP Address that the packets will be attempting to access.
- **Netmask**: Specify which portion of the Destination IP signifies the network trying to be accessed, and which part signifies the packets to which the host will be routed.

Note: 255.255.255.255 is used to signify only the host that was entered in the Destination IP field.

- A **Gateway** of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN. Enter **Gateway** Specifies the next hop to be taken if this route is used.
- Select the **Interface** LAN or WAN, that the IP packet must use to transit out of the router when this route is used.
- **Metric**: If there is only one router between your network and the Destination network, then the Metric value will be 1. This represents the amount of hops it will take to reach the Destination IP or network. A hop is considered to be traffic passing through a router from one network to another.
- **Save Settings:** click to save this information and continue.

Route List:

The **Route List** shows the current routing table entries and certain required routes are predefined and cannot be changed. By toggling the **Enable** checkbox, the Rule List can be enabled or disabled. To edit the entries, click on the pencil icon. To delete the entries click on the trash can icon. If you have made some changes or deletions, click Save **Settings** at the top of the page. If your configuration settings are over then click the Reboot the Device button otherwise click Continue. The router must reboot before new settings will take effect.

8.6 Access Control:



The Access Control option allows you to control access in and out of your network. Use this feature to grant access only to approved sites, limit web access based on time or dates, and/or block Internet access for applications like P2P utilities or games.

Enabled:

By default, the Access Control feature is disabled. When Access Control is disabled, every device on the LAN is permitted to access the Internet. If Access Control is enabled, every device on the LAN that needs to access the Internet must have an Access Control rule that explicitly permits it to access the Internet. Devices that do not have an Access Control Rule cannot access the Internet. When Access Control is enabled, through Policy Wizard you can enter information:

Policy Wizard:

- Click **Add Policy**



Add New Policy:

- Click **Next** to continue.

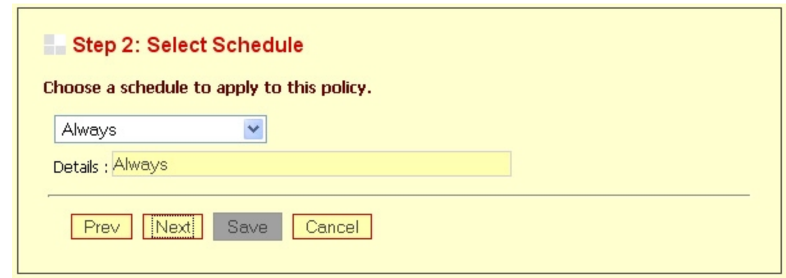
Step 1: Choose Policy Name:

- **Policy Name.** Typically, this would be a system name or user name such as "John's Computer."
- Click **Next** to continue.



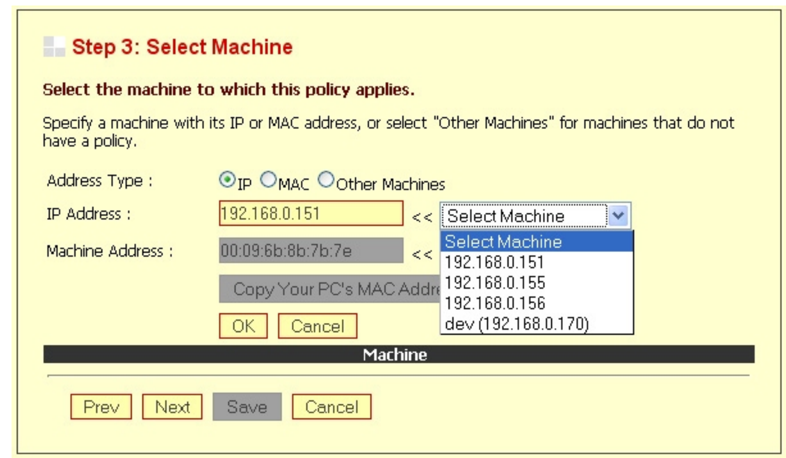
Step 2: Select Schedule:

- Select the **Schedule** of times when you want the policy to apply. If you do not see the schedule you need in the list of schedules, Go to the Tools > Schedules screen and create a new schedule.
- Click **Next** to continue.



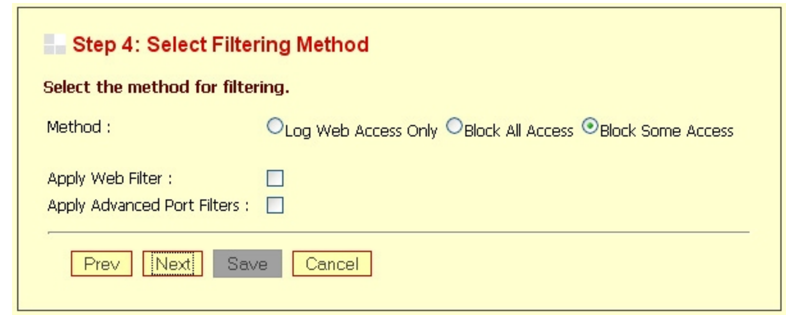
Step 3: Select Machine:

- Select **Address Type** from **IP, MAC, or Other Machines** to apply this rule to the corresponding address type.
- Enter or select the local network **IP Address** of the machine that you want the access control rule to apply to.
- Enter or select the **Machine Address** of the machine that you want the access control rule to apply to.



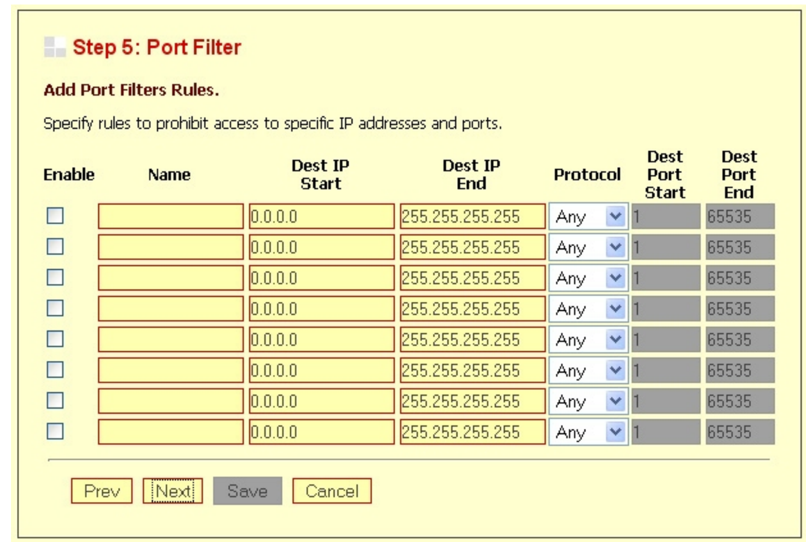
Step 4: Select Filtering Method:

- **Apply Web Filter:** With this option is enabled, the specified system will only have access to the Web sites listed in the Web filter section.
- **Log Internet Access:** When this option is enabled, all of the Web sites visited by the specified machine will be logged.
- **Filter Ports:** When this option is enabled, you can specify that the rule enables access only to specific IP addresses and ports.



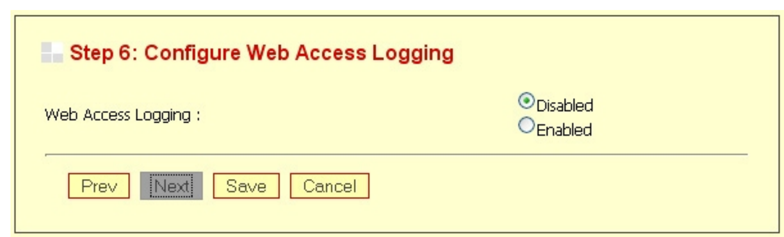
Step 5: Port Filter:

- Click on the Enable Check Box.
- Enter the Name of the Filter.
- Enter the Starting Destination IPAddress..
- Enter the Ending Destination IPAddress.
- Select the protocol.
- Enter the Starting Destination Port.
- Enter the Ending Destination Port.
- Click **Next** to continue.



Step 6: Configure Web Access Logging:

- **Save:** click to save this information and continue.
- Click **Next** to continue.



8.7 Web Filter:



The Web Filter options allows you to set-up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all other Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

The Web Filter section is where you add the Web site to be used for Access Control.

Add/Edit Web Site:

- When the **Enable** checkbox is checked, entries in the Allowed Web Site List can be activated or deactivated with these new entries are activated by default.
- Enter the URL (address) of the **Website** that you want to allow. Enter the most inclusive domain name. Many websites construct pages with images and content from other sites. If you do not enable all of the web sites used to construct a page access will be forbidden. For example, to access my.yahoo.com, you must enable access to yahoo.com, yimg.com, and doubleclick.net.
- **ADD:** click to save this information and continue.

Allowed Web Site List:

This section lists the currently allowed web sites. By toggling the **Enable** checkbox Allowed Web Site List can be enabled or disabled. To edit the entries click on the pencil icon. To delete the entries click on the trash can icon. If you have made any changes or deletions, click on **Save Settings** at the top of the page. If your configuration settings are complete, click **Reboot the Device** or click **Continue**. The router must reboot before new settings will take effect.

8.8 MAC Address Filters:



The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

Filter Settings:

When the **MAC Address Filter** is **Enabled**, depending on the mode selected, computers are granted or denied network access based on their MAC address.

- Select the **Mode** from the drop-down list**.** If **Allow** is selected, only computers with MAC addresses listed in the MAC Address List are granted network access and if you select **Deny**, any computer with a MAC address listed in the MAC Address List are granted network access.
- When **Filter Wireless Clients** is selected, the MAC address filters will be applied to wireless network clients.
- When **Filter Wired Clients** is selected, the MAC address filters will be applied to wired network clients.

Add MAC Address

- MAC address entries are activated or deactivated with the **Enable** checkbox checked or unchecked.
- Enter the **MAC Address** of the desired computer or connect to the router from the desired computer and click **Copy Your PC's MAC Address** button.
- **ADD:** click to save this information and continue.

MAC Address List:

This section lists the current MAC address filters. By toggling the **Enable** checkbox the MAC Address List can be enabled or disabled. To edit the entries click on the pencil icon. To delete the entries click on the trash can icon. If you have made any changes or deletions, click on **Save Settings** at the top of the page. If your configuration settings are complete, click **Reboot the Device** or click Continue. The router must reboot before new settings will take effect.

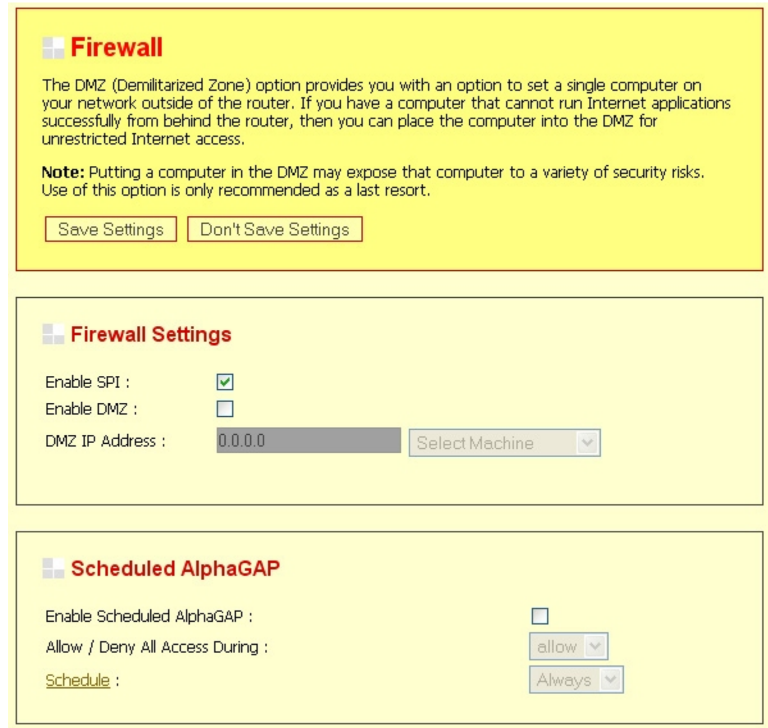
8.9 Firewall:

The DMZ (Demilitarized Zone) option provides you with an option to set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you may place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

- **Enable SPI:** When checked, the extra state information will be reported on the Status > Active sessions page.
- Stateful Packet Inspection (SPI) also known as dynamic packet filtering helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.
- **Enable DMZ means** that computer may expose to a variety of security risks. Use of this option is only recommended as a last resort.

If you have made any changes or deletions, click on **Save Settings** at the top of the page. If your configuration settings are complete, click **Reboot the Device** or Click Continue. The router must reboot before new settings will take effect.



8.10 Scheduled AlphaGAP:

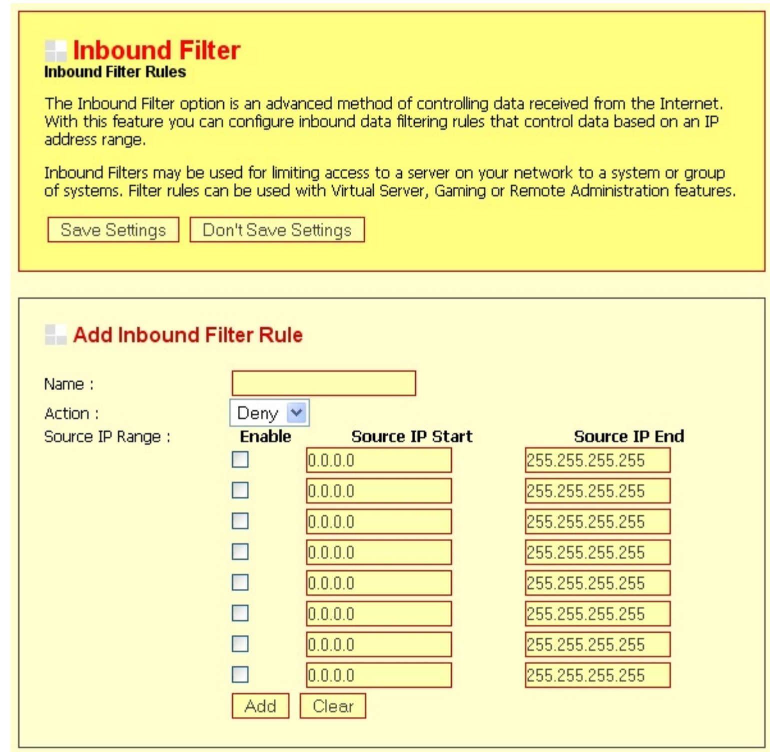
AlphaGAP® Technology ensures that access to the connected computer system is disabled by creating a virtual GAP (disconnection) following a pre-determined Internet idle interval (15 minutes). To enable this security option, check the box titled **Enable Scheduled AlphaGAP®**. Once this option is selected, your Internet connection will automatically disconnect after being idle for 15 consecutive minutes. For more information on AlphaGAP's® effective protection technique, please see AlphaGAP® in our glossary, or visit our website at www.alphashield.com

To set a specified time to deny or allow access on your network, select your appropriate option from the ***Allow/Deny all Access During*** down menu.

8.11 Inbound Filters:

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters may be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming or Remote Administration features.



Add Inbound Filter Rule:

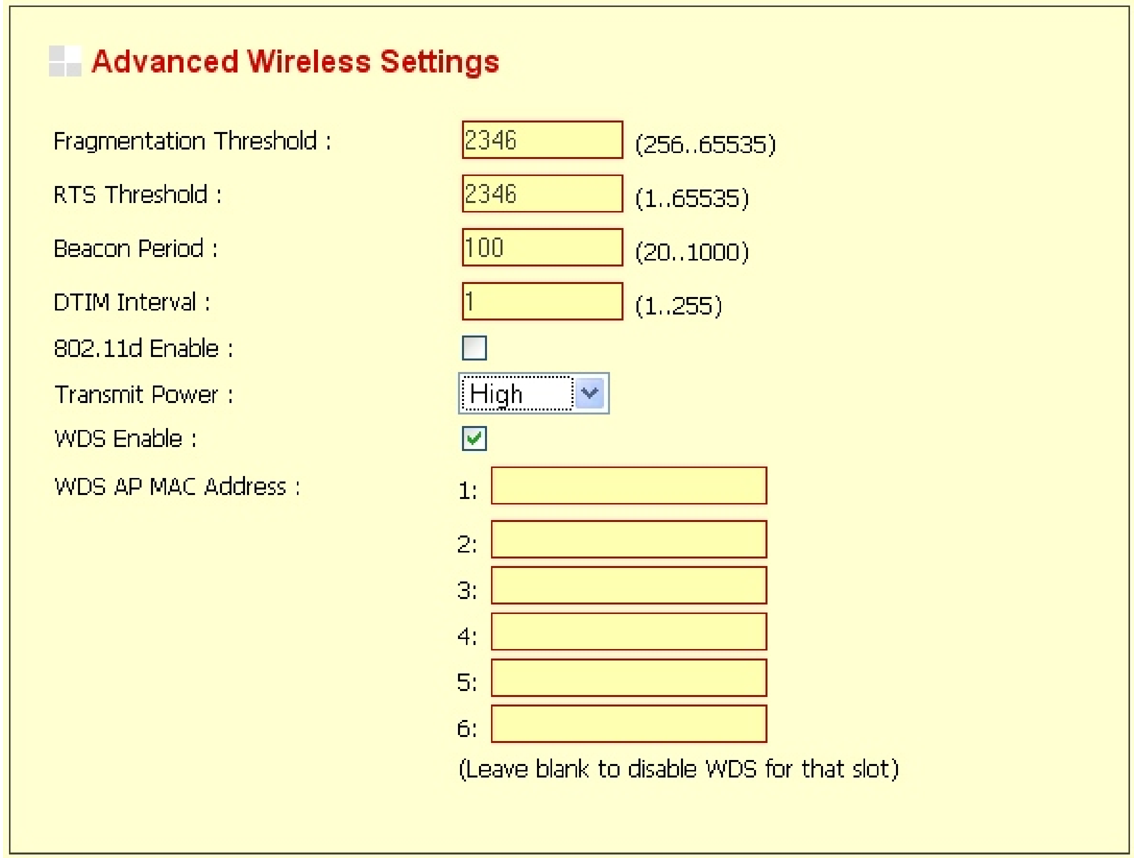
- **Name:** Choose a name for the rule that is meaningful to you.
- **Action:** Here, the inbound filter rule can be set to either allow or deny applicable messages.
- **Source IP Range:** Determines the range of Internet addresses the inbound filter rule applies to.
- **Source Port Range:** Determines the range of ports in which the inbound filter rule applies to.
- **Public Port Range:** Determines the range of WAN side ports associated with the servers on the LAN that the inbound filter rule applies to.

Inbound Filter Rules List:

This section lists the current Inbound Filter rules. By toggling the **Enable** checkbox, the MAC Address List can be enabled or disabled. To edit the entries click on the Pencil icon. To delete the entries, click on the trash can icon. If you have made some changes or deletions click on **Save Settings** button on top of page. If you have made any changes or deletions, click on **Save Settings** at the top of the page. If your configuration settings are complete, click **Reboot the Device** or click Continue. The router must reboot before new settings will take effect.

8.12 Advanced Wireless:

Advanced Wireless Settings:

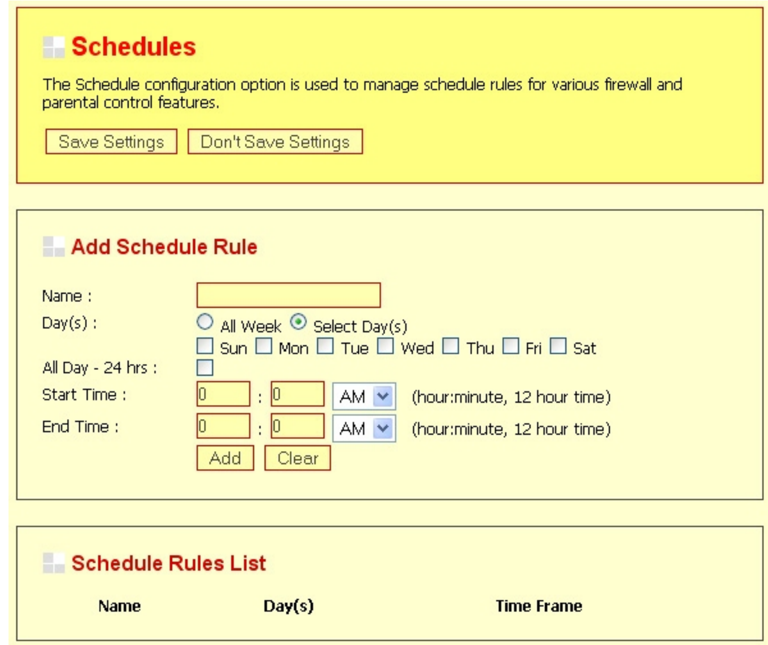


- The default setting of the **Fragmentation Threshold** should remain 3200. Setting the Fragmentation value too low may result in poor performance. If you may slightly adjust your Fragmentation value somewhere in the between the recommended range of 256 to 3200.
- The default setting of the **RTS Threshold** should remain of 3200. If you encounter inconsistent data flow, only minor modifications to the value are recommended.
- Specify **Beacon Period** value between 20 and 1000. The default value is set to 100 milliseconds.
- The default value **DTIM Interval** is set to 1. Valid settings are between 1 and 255.
- **802.11d Enable checked** enables 802.11d operation; the feature should only be enabled if you are in a country that requires it. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11standard.
- When **WDS Enable** is enabled, this access point functions as a wireless bridge and is able to wirelessly communicate with Other AP's via WDS links.

Note: WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bidirectional so this AP must know the MAC address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP (the router).

- Specifies one-half of the **WDS AP MAC Address**. The other AP must also have the MAC address of this AP (the router) to create the WDS link back to the router.

8.13 Schedules:



The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

Add/Edit Schedule Rule:

- Enter the **Schedule Name.**
- To select the **Day(s)** Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.
- Select **All Day** option to make this schedule in effect all day for the selected day(s).
- If you don't use the All Day option, then you enter the time in **Start Time**. Enter the hour in first box and the minute in the second box. Email events are triggered only by the start time.
- **End Time:** The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not used for email events.
- Once you are finished with the Rule Scheduling, you must click the **Add** button to create the schedule.
- When you finish Adding the settings, you must click the **Save Settings** button at the top of the page to make the changes effective and permanent.

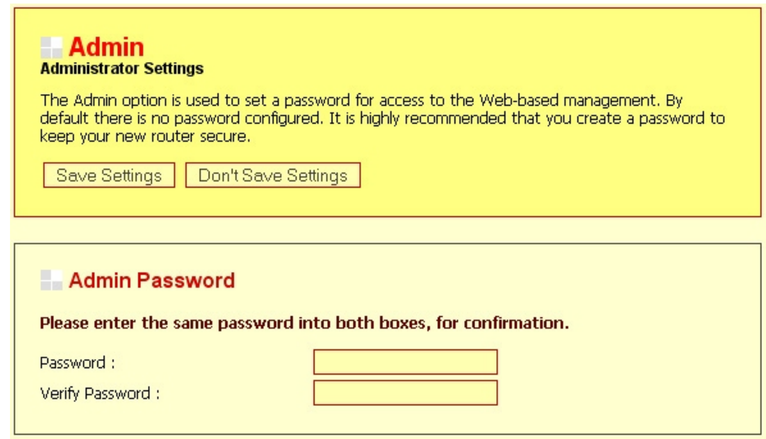
Schedule Rules List:

This list displays all of the currently defined schedules. By toggling the **Enable** checkbox schedules rule List can be enabled or disabled. To edit the entries click on the pencil icon. To delete the entries click on the trash can icon. If you have made any changes or deletions, click on **Save Settings** at the top of the page. If your configuration settings are complete, click **Reboot the Device** or click Continue. The router must reboot before new settings will take effect.

9 TOOLS:

9.1 Admin:

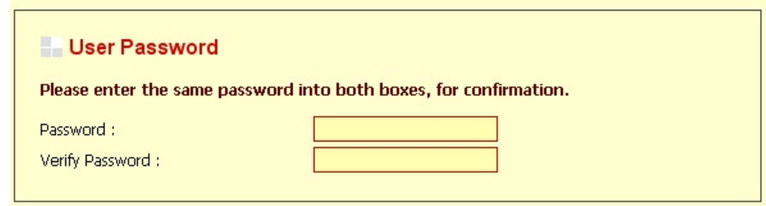
The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new router secure.



Admin Password

To Set Admin Password

- Enter a Password of your choice
- To **Verify your Password,** re-enter it below

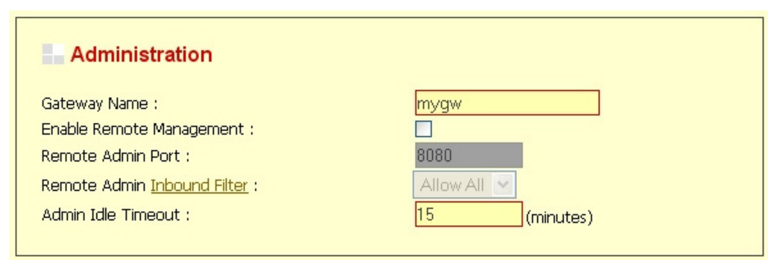


User Password

(Only required if you want to limit a user from having Administrator rights)

To Set your User Password

- Enter a Password of your choice
- To **Verify your Password,** re-enter it below



Administration:

- Enter or change **the Gateway Name** of the router.
- Enabling **Enable Remote Management** allows to manage the router from anywhere with an Internet connection.
- The **Remote Management Server Port** will be accessed from the Internet.
- When there is no activity before the administration session is closed that amount of time is **Admin Idle Timeout .**

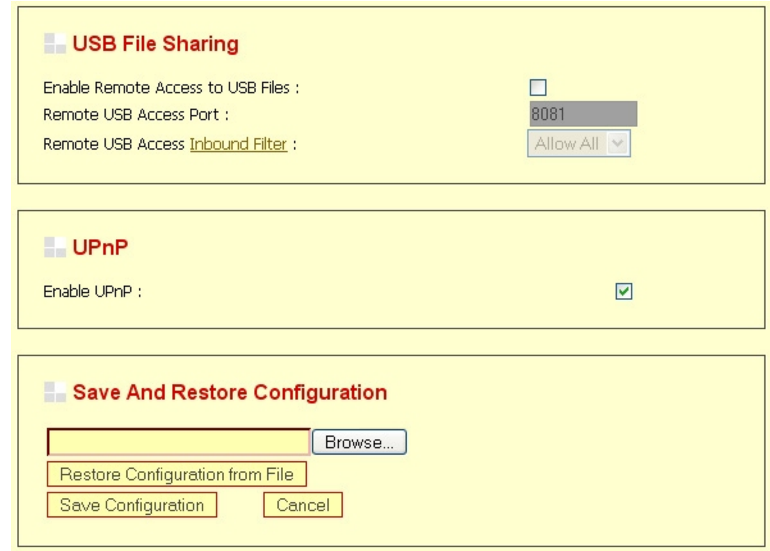
USB File Sharing:

- Select **Enable Remote Access to USB files** to allow the Remote User to access the USB files.
- Select the port that you want the Remote User e.g. 8081
- Select the **USB Access Inbound Filer** to allow the Remote user to access files.

UPnP:

- Select the **Enable UPnP**

Note: You need to have the UPnP selected for the Router to be able to communicate with the network.

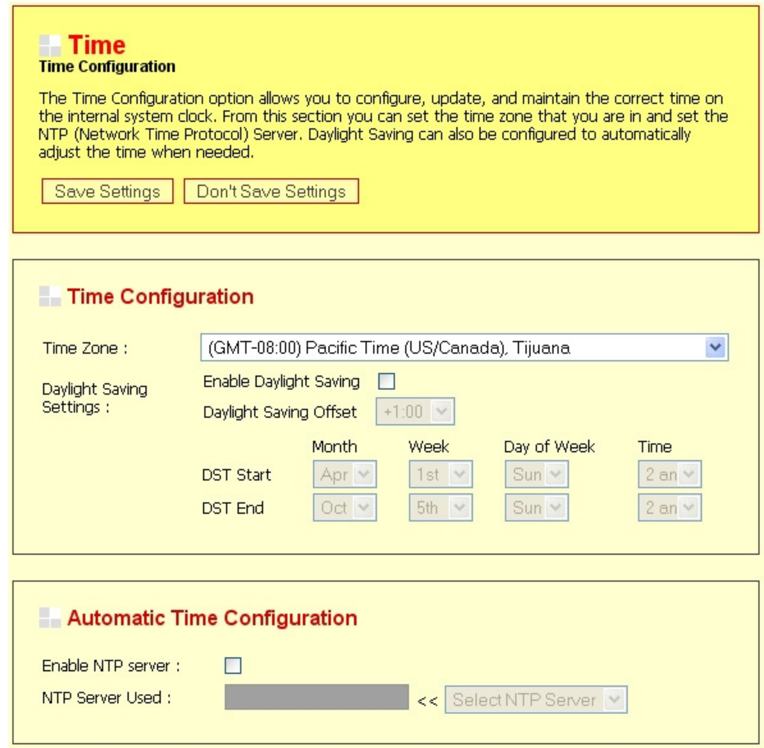


Save and Restore Settings:

- To load previously saved router configuration settings click on **Restore Settings button.**
- To save the router configuration to a file on your computer Click on **Save Settings**.

9.2 Time:

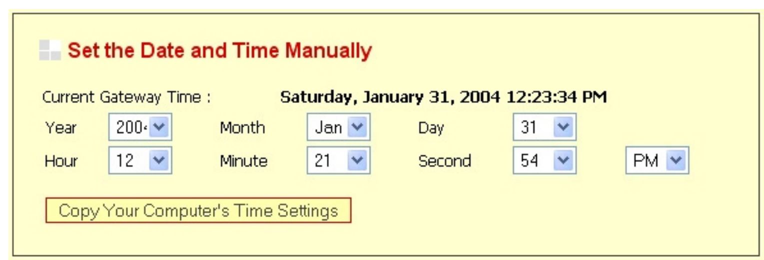
The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set your local time zone and set the Time Server. Daylight Saving Settings can also be configured to automatically adjust the time when needed.



Time Configuration:

- Select your local time zone from the **Time Zone** pull down menu.
- Check **Daylight Saving Enable** if your location observes daylight saving time.
- Select **Daylight Saving Offset** if your location observes daylight saving time.
- Select **Synchronize time with NTP server** if you want the router's clock synchronized to a Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate
- Select an **NTP Server** from the list for synchronization or type in the address of a time server.

Set the Date and Time



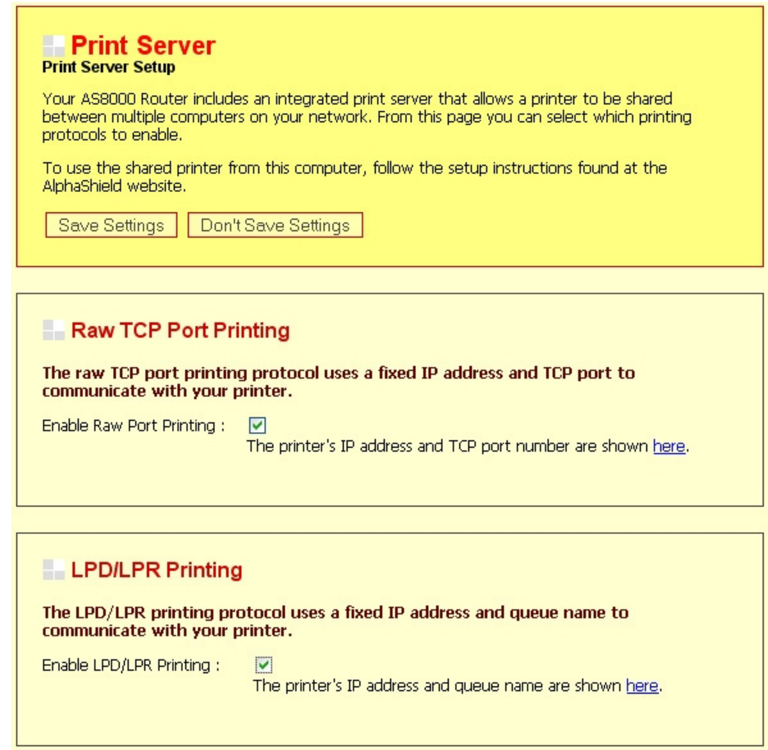
- If you do not have the NTP Server option in effect, you can either manually set the time for your router here or you can click **Copy Your Computer's Time Settings** to the time from the computer you are using.
- If the router loses power for any reason, it cannot keep its clock running and will not have the correct time when it is started again. To maintain the correct time for schedules and logs, you must enter the correct time after you restart the router or you must enable the NTP Server option.

9.3 Print Server Setup:

Your AlphaShield Router includes an integrated print server that allows a printer to be shared between multiple computers on your network. From this page you can select which printing protocols to enable.

To use the shared printer from this computer, follow the setup instructions found at the AlphaShield website.

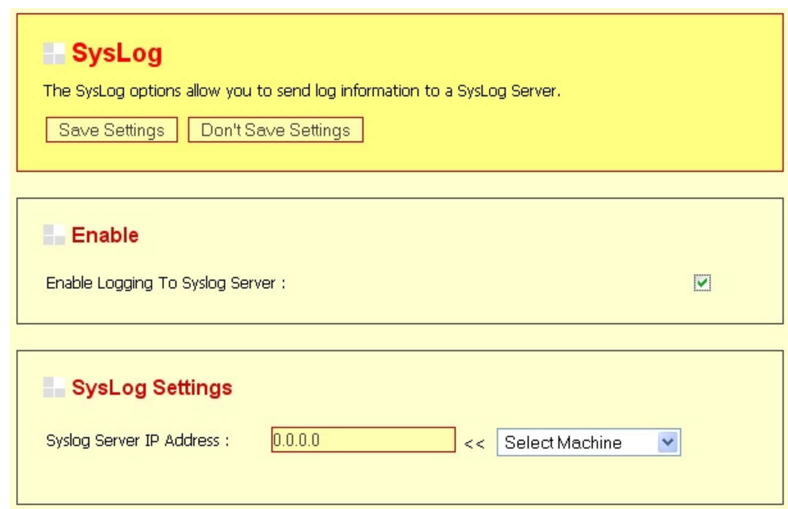
- Please select **Enable Raw Port Printing** and/or **LPD/LPR Printing**, This will enable the Router to find and communicate with the connected printer.
- Please install the printer in your computer as Local printer on the TCP/IP port. The Port IP address is same as the IP address of your Router e.g. 192.168.0.1 The Port address is 9100.



9.4 Syslog:

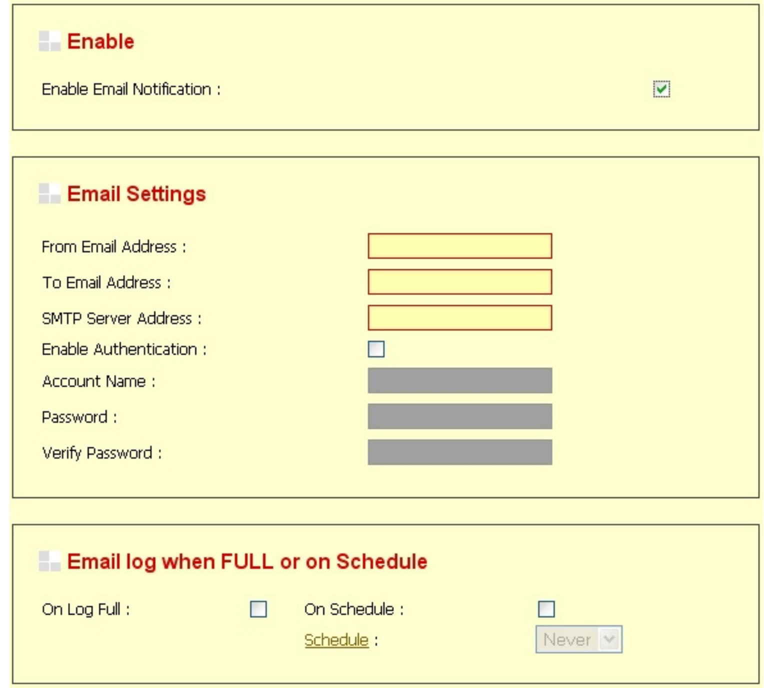
This section allows you to archive your log files to a Syslog Server.

- **Enable: Enable Logging To Syslog Server** to output the router logs to a Syslog Server on your network.
- **Syslog Settings: Enter the Server IP Address** of the Syslog Server.



9.5 Email:

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.



Email Settings:

- **From Email address: Enter the address** that will appear as the sender when you receive a log file or firmware upgrade notification via email.
- **To Email address: Enter the address** where you want the email sent.
- **SMTP Server Address: Enter the address** for sending email.
- **Enable Authentication**: Check box to authenticate SMTP server.
- **Account Name: Enter the account name** for sending email.
- Enter the Password associated with this email.
- To **Verify your Password,** re-enter the password.

Email Log When Full or on Schedule

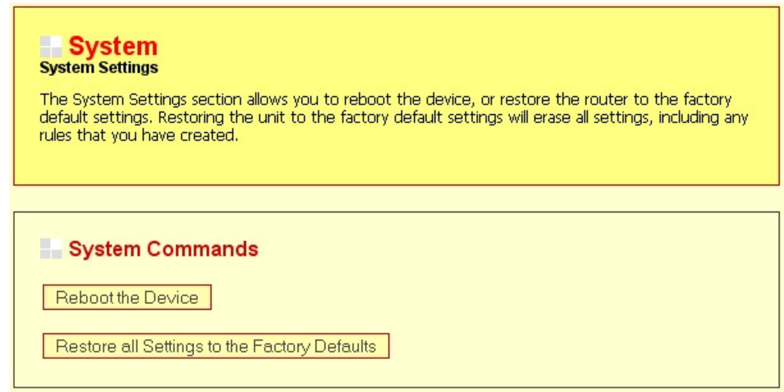
- When **On Log Full** is selected, logs will be Sent via email when the log is full.
- Selecting **On Schedule** will send the logs via email according to schedule.
- **Schedule** is enabled when **On Schedule** is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to Tools > Schedules

9.6 System:

The System Settings section allows you to reboot the device or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings including any rules that you've created.

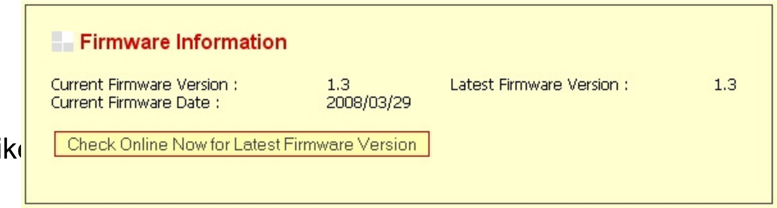
System Commands:

- To restart the router click on **Reboot the Device**.
- To restore all configuration settings back to the factory defaults click on **Restore all Settings to the Factory Defaults**. You can save router configuration settings from the Admin page. Any settings that have not been saved will be lost.

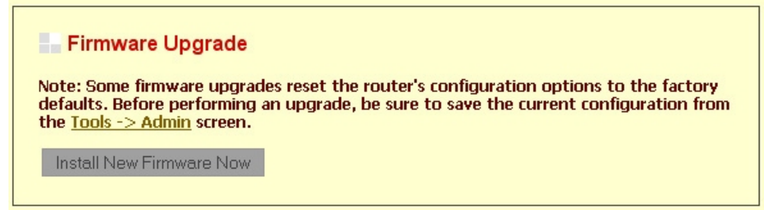


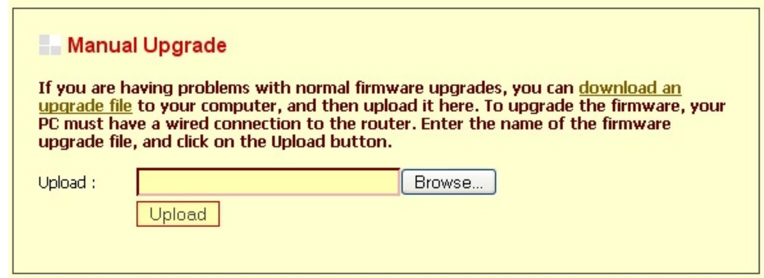
9.7 Firmware:

The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance. To check for the latest firmware, click the **Check Online Now for Latest Firmware Version** button. If you would like to be notified when new firmware is released, place a checkmark in the box next to Email Notification of Newer Firmware Version.



The Firmware Upgrade section can be used to update your router to the latest firmware code to improve functionality and performance. To check for the latest firmware, click the Check Online Now button. If you would like to be notified when new firmware is released, place a checkmark in the box next to Email Notification of Newer Firmware Version.





Firmware Information:

- ✍ To check for the latest firmware, click **Check Online Now for Latest Firmware Version.**

Firmware Upgrade:

- ✍ Click the **Browse** button to locate AlphaShield upgrade file on your computer.
- ✍ Once you have found the file to be used, click the **Upload** button below to start **the firmware upgrade** process.



Manual Upgrade

- ✍ Wait for the router to reboot.
- ✍ Confirm updated firmware revision on status page.

Firmware Upgrade Notification Options:

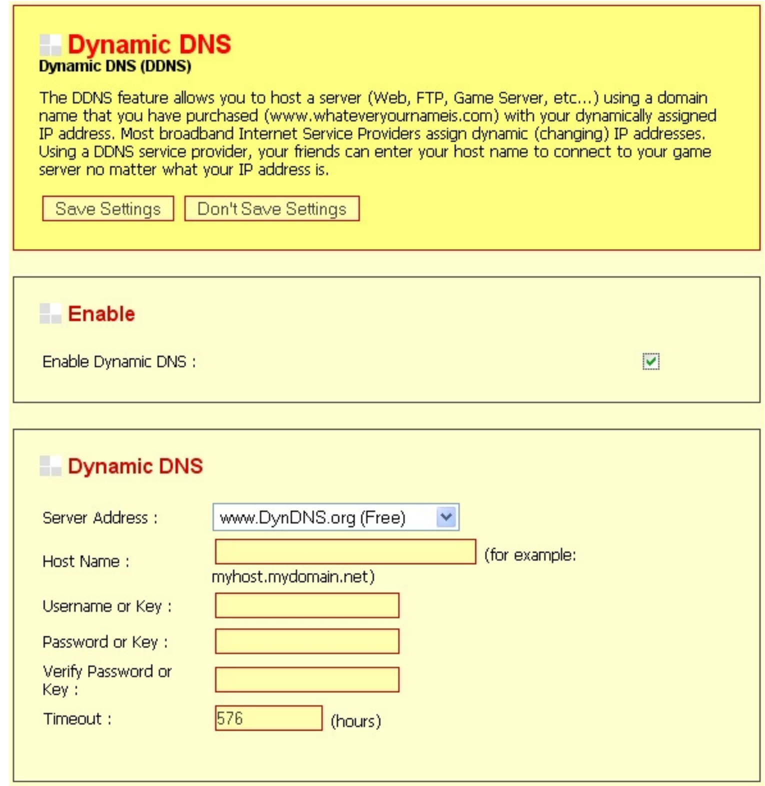
- ✍ To make router check online periodically to see if a newer version of the firmware is available enable **Automatically Check Online for Latest Firmware Version**.
- ✍ When **Email Notification of Newer Firmware Version** is enabled, an email will be sent to the email address configured in the email section whenever new firmware Is available.

9.8 Dynamic DNS:

Dynamic DNS allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

If you have purchased your own domain name and registered with a dynamic DNS service provider enable Dynamic **DNS**.

- Select **Server Address** from the pull-down list.
- Enter **Host Name**.
- Enter the **Username or Key** provided by your service provider.
- Enter the **Password or Key** provided by your service provider.
- To **Verify Password or Key** re-type the password or key provided by your service provider.
- Enter **Timeout** period is entered in hours. **Timeout is** the time between periodic updates to the Dynamic DNS, if your dynamic IP address has not changed.



Note: This option will disable it self if Username and Password or keys are incorrect.

10. STATUS:

The Status items are mainly informational.

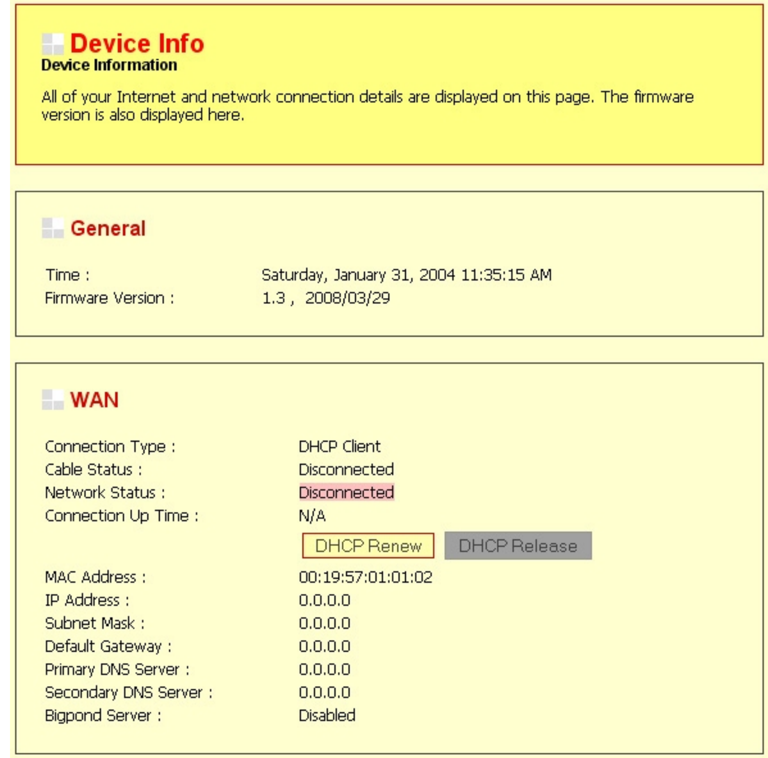
10.1 Device Info:

General:

- **Time option** displays the time and date that the router is set to.
- **Firmware Version option** displays the currently loaded firmware version.

WAN:

- **Connection Type shows t**he Internet connection type that is being used.
- **MAC Address** is seen over the Internet.
- **IP Address** being used on the WAN port.
- **Subnet Mask** used on the WAN port.
- **Default Gateway** of the WAN port.
- **Primary DNS Server shows the** Primary DNS Server address.
- **Secondary DNS Server shows t**he Secondary DNS Server address.

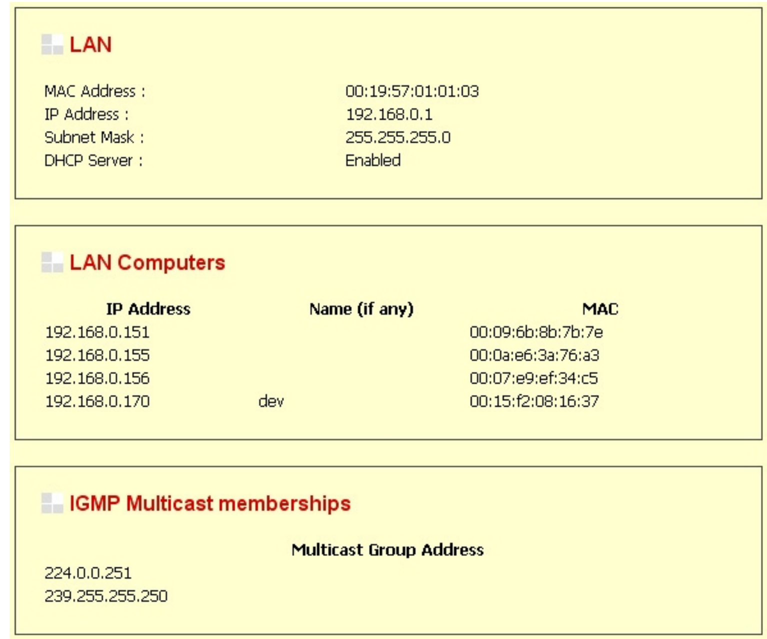


LAN:

- **MAC Address** displayed for your local area network.
- **IP Address** displays the router on your local area network.
- **Subnet Mask** displays the router on your local area network.
- **DHCP Server i**ndicates if the router is acting as a DHCP server on the local area network.

Wireless LAN:

- **Wireless Radio** Indicates whether wireless networking is on or off.
- **MAC Address** displayed for your wireless network.
- **Network Name (SSID)** shows name of your wireless network.
- **Channel** shows the channel being used by the router for broadcasting on the Wireless network.
- **Turbo Mode** indicates whether Turbo Mode is enabled or disabled.
- **Security Type** indicates the type of wireless security being used.



10.2 Wireless:

Use this option to view the wireless clients that are connected to your wireless router.

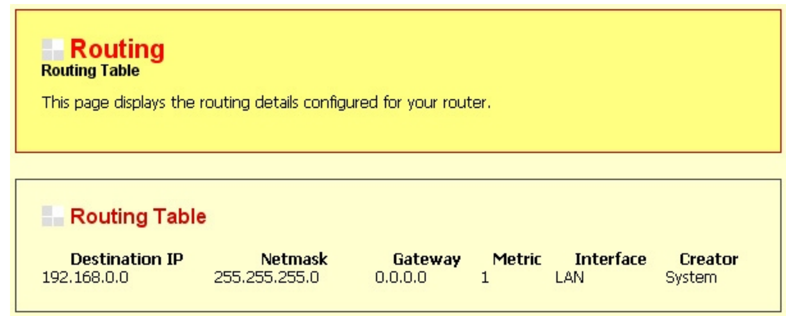
Number Of Wireless Clients

This display includes the number of clients that are connected to the router, the **MAC address** of each system connecting wirelessly, and the **IP address** of Each system connecting wirelessly.



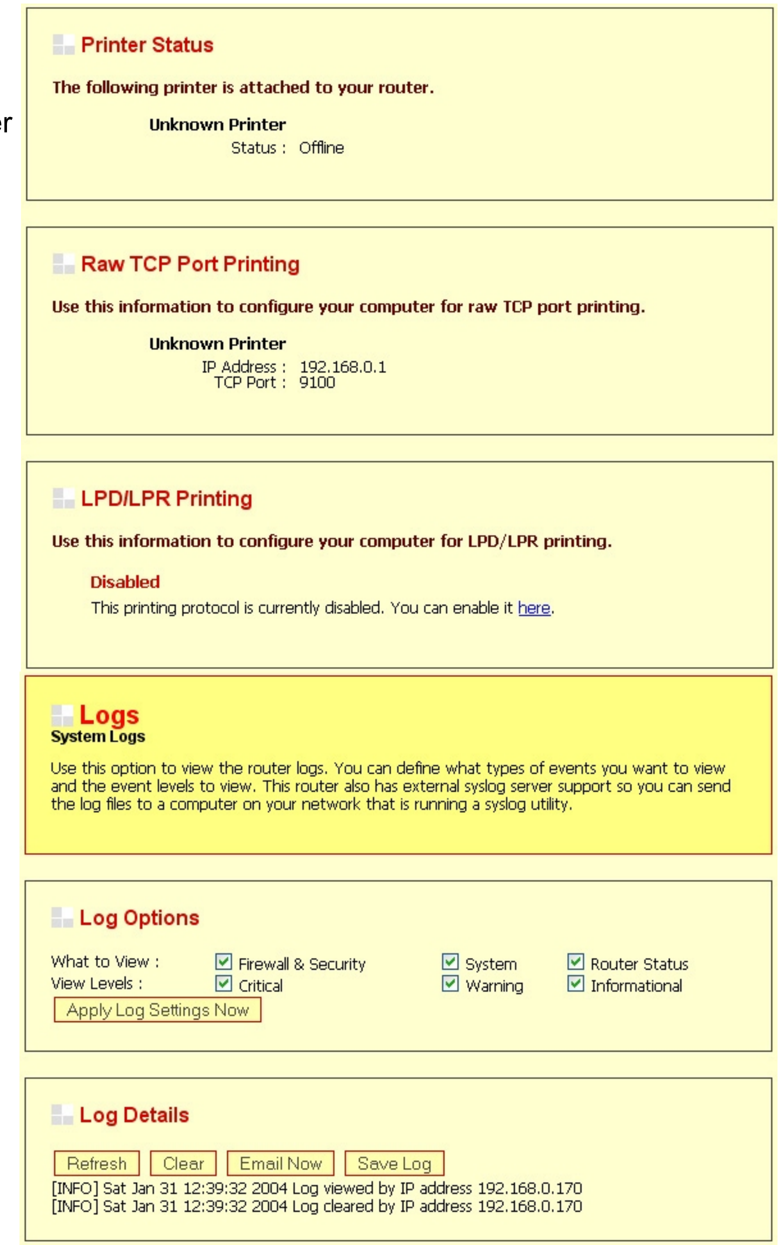
10.3 Routing Table:

- A **Gateway** value of 0.0.0.0 means there is no next hop.
- The **IP address** is directly connected to the router on the interface specified, LAN or WAN.
- A value of 0.0.0.0 in both the **Destination IP** and **Netmask** means that this is the default route.



10.4 Print Server Status:

Your AlphaShield Router includes an integrated print server that allows a printer to be shared between multiple computers on your network. This page displays status information about the print server and any attached printer.



10.5 Logs:

Events are automatically logged (recorded) on your router's internal memory. When the memory is full, old event will be deleted and newer ones will be logged. The router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

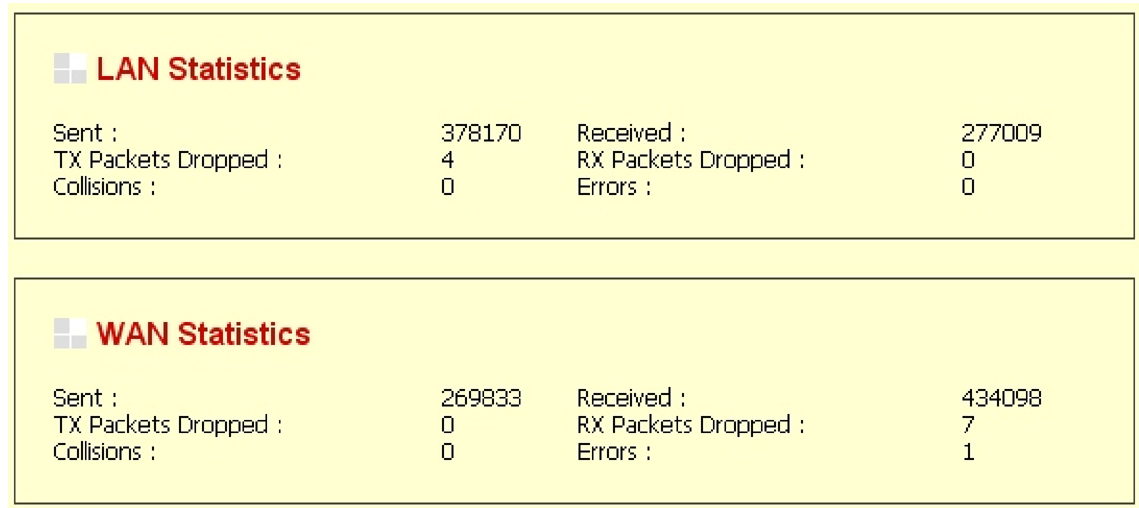
Log Options:

- **What to View** select the type(s) of messages that you want to display from the log.
- **View Levels** select the level(s).
- Click **Apply Log Settings Now** to Continue.

Log Details

- To refresh the log contents click **Refresh.**
- To clear all of the log contents click **Clear**.

10.6 Statistics:



Network Traffic Stats:

Traffic Statistics: Displays packets passing through your router.

Refresh Statistics: Updates the screen with the latest router statistics.

Clear Statistics: Clears all of the values on the screen.

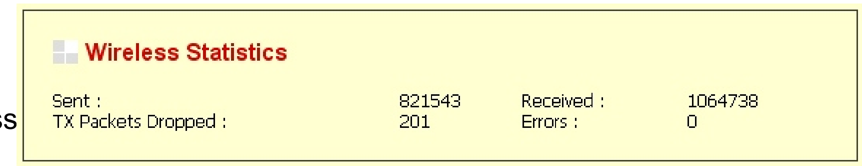
LAN Statistics:

- **Sent** shows the number of packets transmitted to the local area network.
- **Received** shows the number of packets received from the local area network.
- **TX Packets Dropped** shows the number of Transmit Packets dropped on the local area network.
- **RX Packets Dropped** shows the number of receive packets dropped on the local area network.
- **Collisions** shows the number of collisions on the local area network.
- **Errors** shows the number of errors occurring on the local area network.

WAN Statistics:

- Sent shows the number of packets transmitted to the Internet.
- **Received** shows the number of packets received from the Internet.
- **TX Packets Dropped** shows the number of transmit packets sent to the WAN port that were dropped.
- **RX Packets Dropped** shows the number of receive packets sent to the WAN port that were dropped.
- **Collisions** shows the number of collisions involving packets intended for the WAN port.
- **Errors** shows the number of errors occurring with packets intended for the WAN port.

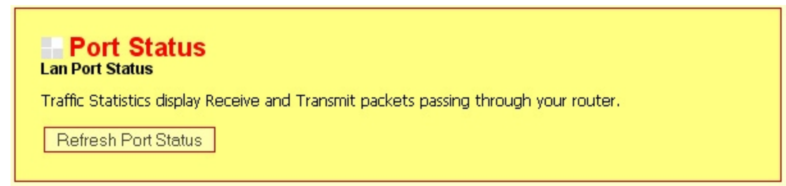
Wireless Statistics:

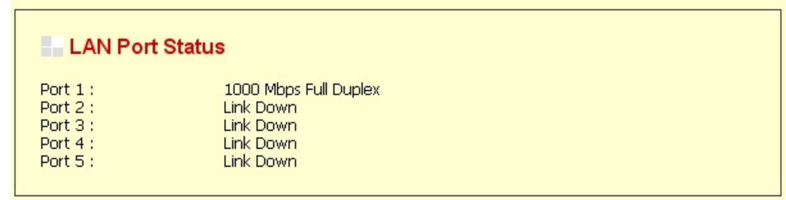


- **Sent** shows the number of packets sent to the wireless network.
- **Received** shows the number of packets received from the Wireless Network.
- **TX Packets Dropped** shows the amount of transmit packets dropped.
- **Errors** shows the number of errors relating to packets to/ from the Wireless Network.

10.7 LAN Port Status:

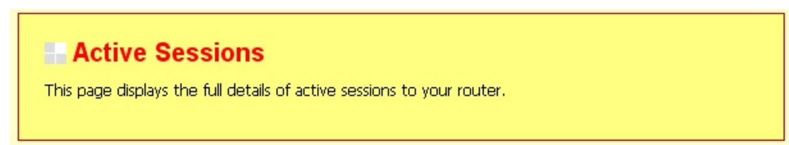
Traffic Statistics simply displays Receive and Transmit packets passing through your router.

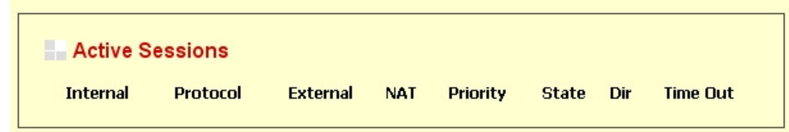




10.8 Active Sessions:

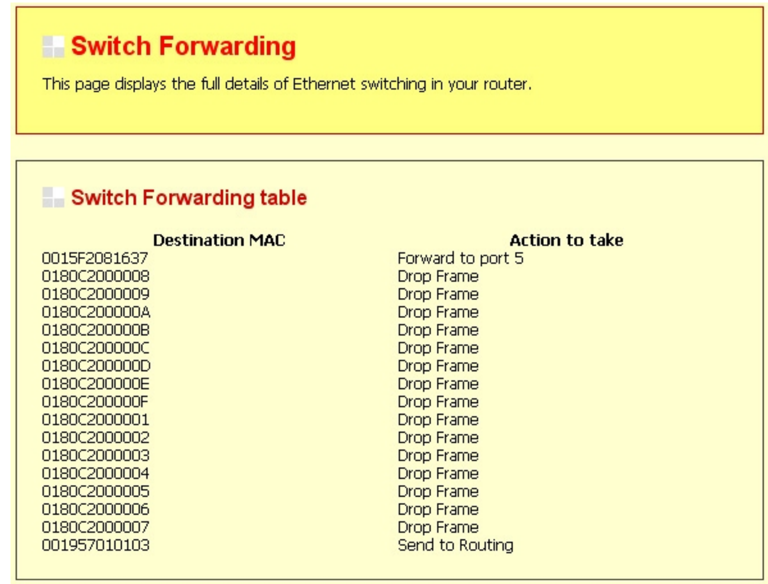
The Active Session page displays the full details of active sessions to your router.





10.9 Switch Forwarding:

This page displays the full details of Ethernet switching in your router.



Switch Forwarding

This page displays the full details of Ethernet switching in your router.

Switch Forwarding table

Destination MAC	Action to take
0015F2081637	Forward to port 5
0180C2000008	Drop Frame
0180C2000009	Drop Frame
0180C200000A	Drop Frame
0180C200000B	Drop Frame
0180C200000C	Drop Frame
0180C200000D	Drop Frame
0180C200000E	Drop Frame
0180C200000F	Drop Frame
0180C2000001	Drop Frame
0180C2000002	Drop Frame
0180C2000003	Drop Frame
0180C2000004	Drop Frame
0180C2000005	Drop Frame
0180C2000006	Drop Frame
0180C2000007	Drop Frame
001957010103	Send to Routing

11. GLOSSARY:

Access Control List - ACL. Database of network devices that are allowed to access resources on the network.

Access Point - AP. Device that allows wireless clients to connect to it and access the network

Ad-hoc network - Peer-to-Peer network between wireless clients

Address Resolution Protocol - ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

ADSL - Asymmetric Digital Subscriber Line

Advanced Encryption Standard - AES. Government encryption standard

AlphaGAP® the first of its kind in the security market, which allows the user to physically or logically disconnect or reconnect seamlessly

Alphanumeric - Characters A-Z and 0-9

Antenna - Used to transmit and receive RF signals.

AppleTalk – A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol – AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer - 7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII - American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation – The loss in strength of digital an analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication – To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing - APIPA. An IP address that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

Backward Compatible - The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth - The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System – BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud – Data transmission speed

Bit rate – The amount of bits that pass in given amount of time

bit/sec – bits per second

BOOTP – Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck – A time during processes when something causes the process to slowdown or stop all together

Broadband – A wide band of frequencies available for transmitting data

Broadcast – Transmitting data in all directions at once

Browser – A program that allows you to access resources on the web and provides them to you graphically

Cable modem – A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

Card Bus – A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

Carrier Sense Multiple Access/Collision Avoidance – CSMA/CA

Carrier Sense Multiple Access/Collision Detect – CSMA/CD

CAT 5 – Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client – A program or user that requests data from a server

Collision – When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie – Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD – Carrier Sense Multiple Access/Collision Detection

Data – Information that has been translated into binary do that it can be processed or moved to another device

Data Encryption Standard – Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Data-Link layer – The second layer of the OSI model. Controls the movement of data on the physical link of a network

Database – Organizes information so that it can be managed and updated, as well as easily accessed by users or applications. DB-25 – A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9 – A 9 pin connector for RS-232 connections

dBd - decibels related to dipole antenna

dBi - decibels relative to isotropic radiator dBm - decibels relative to one milliwatt

Decrypt – To unscramble an encrypted message back into plain text

Default – A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone – DMZ. A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP – Dynamic Host Configuration Protocol. Used to automatically assign IP addresses from a predetermined pool of addresses to computers or devices that requests them

Digital certificate – An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum – DSSS. Modulation technique used by 802.11b wireless devices

DNS – Domain Name System. Translates Domain Names to IP addresses

DOCSIS – Data Over Cable Service Interface Specifications. The standard interface for cable modems

Domain name – A name that is associated with an IP address

Download – To send a request from one computer to another and have the ?le transmitted back to the requesting computer

DSL – Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex – Sending and Receiving data transmissions at the sane time

Dynamic DNS service – DDNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports DDNS, whenever the IP address changes

Dynamic IP address – IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

EAP – Extensible Authentication Protocol

Email – Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption – Converting data into hypertext so that it cannot be easily read

Enterprise – Large organizations that use computers

Ethernet – The most widely used technology for Local Area Networks.

Fiber optic – A way of sending data through light impulses over glass or plastic wire or fiber

File server – A computer on a network that stores data so that the other computers on the network can all access it

File sharing – Allowing data from computers on a network to be accessed by other computers on the network will different levels of access rights

Firewall – A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware – Programming that is inserted into a hardware device that tells it how to function

Fragmentation – Breaking up data into smaller pieces to make it easier to store

FTP – File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex – Sending and Receiving data at the same time

Gain – The amount an ampli?er boosts the wireless signal

Gateway – A device that connects your network to another, like the internet

Gbps – Gigabits per second

Gigabit Ethernet – Transmission technology that provides a data rate of 1 billion bits per second

Graphical user interface – GUI

H.323 – A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices Half-duplex – Data cannot be transmitted and received at the same time

Hashing – Transforming a string of characters into a shorter string with a prede?ned length

Hexadecimal – Characters 0-9 and A-F

HomePNA – Networking over telephone lines

Home R.F. – Networking standard that combines 802.11b and DECT (Digital Enhanced Cordless Telecommunication) that provides speeds up to 1.6 Mbps and a distance of 150 ft using a Frequency Hopping transmission method

Hop – The action of data packets being transmitted from one router to another

Host – Computer on a network

HTTP – Hypertext Transfer Protocol is used to transfer ?les from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS – HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub – A networking device that connects multiple devices together

ICMP – Internet Control Message Protocol

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IGMP – Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS – Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE – Internet Key Exchange is used to ensure security for VPN connections

Infrastructure – In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet – A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer – A World Wide Web browser created and provided by Microsoft

Internet Protocol – The method of transferring data from one computer to another on the Internet

Internet Protocol Security – IPSec provides security at the packet processing layer of network communication

Internet Service Provider – An ISP provides access to the Internet to individuals or companies

Interoperability – The ability for products to interact with other products without much customer interaction

Intranet – A private network

Intrusion Detection – A type of security that scans a network to detect attacks coming from inside and outside of the network

IP – Internet Protocol

IP address – A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec – Internet Protocol Security

IPv6 – Internet Protocol Version 6 uses 128-bit addresses and was developed to solve the problem that we face of running our of IP version 4 addresses

IPX – Inter-network Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP – Internet Service Provider

Java – A programming language used to create programs and applets for web pages

Kbps – Kilobits per second

Kbyte - Kilobyte

Kerberos – A method of securing and authenticating requests for services on a network

LAN – Local Area Network

Latency – The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED – Light Emitting Diode

Legacy – Older devices or technology

Local Area Network – A group of computers in a building that usually access files from a server

MAC address – A unique hardware address for devices on a Local Area Network

MDI – Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX – Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

Megabit – Mb

Megabyte – MB

Megabits per second – Mbps

MIB – Management Information Base is a set of objects that can be managed by using SNMP

Modem – A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE – Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU – Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast – Sending data from one device to many devices on a network

NAT – Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI – NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS – Network Basic Input/Output System

Netmask – Determines what portion of an IP address designates the Network and which part designates the Host**NetWare –** A Server Software developed by Novell

Network Interface Card – A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network later – The third layer of the OSI model, which handles the routing of traffic on a network

Network Time Protocol – Used to synchronize the time of all the computers in a network

NIC – Network Interface Card

NTP – Network Time Protocol

OFDM – Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI – Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF – Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

Password – A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network – The interconnection of networking devices within a range of 10 meters

Physical layer – The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

PoE – Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP 3 – Post Office Protocol 3 is used for receiving email

PowerZONE Technology - A proprietary technology developed by AlphaShield's Engineers, which utilizes a bi-directional Wi-Fi signal that increases the receiver sensitivity and transmitted power. This allows it to connect to those hard to reach spots. It can even penetrate concrete walls and other structures that inhibit other standard Wi-Fi reception.

PPP – Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE – Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP – Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble – Used to synchronize communication timing between devices on a network

QoS – Quality of Service

RADIUS – Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Rendezvous – Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater – Retransmits the signal of an Access Point in order to extend it's coverage

RIP – Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11 – The most commonly used connection method for telephones

RJ-45 – The most commonly used connection method for Ethernet

RS-232C – The interface for serial communication between computers and other related devices

RSA – Algorithm used for encryption and authentication

Samba – A freeware program that allows for resources to be shared on a network. Mainly used in Unix based Operating Systems

Server – A computer on a network that provides services and resources to other computers on the network

Session key – An encryption and decryption key that is generated for every communication session between two computers

Session layer – The fifth layer of the OSI model, which coordinates the connection and communication between applications on both ends Simple Mail Transfer **Protocol –** Used for sending and receiving email

Simple Network Management Protocol – Governs the management and monitoring of network devices

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SOHO – Small Office/Home Office

SPI – Stateful Packet Inspection

SSH – Secure Shell is a command line interface that allows for secure connections to remote computers

SSID – Service Set Identifier is a name for a wireless network

Stateful inspection – A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests for incoming packets are allowed to pass though the firewall

Subnet mask – Determines what portion of an IP address designates the Network and which part designates the Host

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TFTP – Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput – The amount of data that can be transferred in a given time period

Traceroute – A utility displays the routes between you computer and specific destination

UDP – User Datagram Protocol UNC – Universal Naming Convention allows for shares on computers to be identified without having to know what storage device it's on

Unicast – Communication between a single sender and receiver

Universal Plug and Play – A standard that allows network devices to discover each other and configure themselves to be a part of the network

UPnP – Universal Plug and Play

URL – Uniform Resource Locator is a unique address for files accessible on the Internet

UTP – Unshielded Twisted Pair

Virtual LAN - Virtual Private Network – A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN – Virtual LAN

Voice over IP – Sending voice information over the Internet as opposed to the PSTN

VoIP – Voice over IP

Wake on LAN – Allows you to power up a computer though it's Network Interface Card

WAN – Wide Area Network

Web browser – A utility that allows you to view content and interact will all of the information on the World Wide Web

WEP – Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wi-Fi – Wireless Fidelity

Wi-Fi Protected Access – An updated version of security for wireless networks that provides authentication as well as encryption

Wide Area Network - A network spanning a large geographical area or consisting of more than one LAN.

Wireless ISP – A company that provides a broadband Internet connection over a wireless connection

Wireless LAN – Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP – Wireless Internet Service Provider

WLAN – Wireless Local Area Network

Yagi antenna – A directional antenna used to concentrate wireless signals on a specific location

12. TECHNICAL SPECIFICATIONS:

Internal Dual Processing	Dedicated 250 MHz High Speed Network Processor Ip3023 Dedicated High Speed Multi-Port Gigabit Switch & Co-Processor SparX-5
Hardware Interfaces	5 x 10/100/1000 Auto-Sensing Gigabit Ethernet LAN Ports MDI/MDI-X 1 x 10/100 Auto-Sensing Fast Ethernet WAN Port MDI/MDI-X 4 x Universal Serial Bus Connections (USB 1.1)
Standard	IEEE 802.11g Wireless Standard IEEE 802.11b Wireless Standard IEEE 802.3 Ethernet Standard 10Mbps IEEE 802.3u Ethernet Standard 100Mbps IEEE 802.3ab Ethernet Standard 1Gbps
Certifications	FCC Part 15, 15.247 15.205, 15.209, IC RSS 139 & RSS 210
Wireless Frequency Range	11 Channels from 2.400 to 2.4835 GHz ISM Band
Wireless Signal Rates	802.11g: 6, 9, 12, 18, 24, 36, 48, 54, 108, Mbps and 108-G Technology with Automatic Fallback 802.11g: 8, 12, 24, 36, 48, 72, 96, 108 Mbps 802.11b: 1, 2, 5.5, and 11 Mbps
Wireless Modulation Technology	802.11b DQPSK, DBPSK, DSSS, CCK Modulation 802.11g BPSK, QPSK, 16QAM, OFDM Modulation
Wireless Transmit Power	Bi-Directional Signal Amplifier Option (Increased Range & Throughput) Transmit +15 dBm to +28 dBm in 10 User Selectable Steps Closed Loop Transmit Power Control (CLTPC) Output + 1dB Receiver Gain -8 dB to +18 dB + 2 dB in 4 User Selectable Steps
Operating Ranges	1300 ft indoor & 3900 ft outdoor
Antennae	Omni-directional dipole 7 dBi External Antenna (Non-Detachable) Omni-directional dipole 3 dBi External Antenna (Non-Detachable)
Antenna Diversity	Polarization Diversity: Switched Linear Vertical and Horizontal Polarization
Security	WEP Encryption 64/128 Wi-Fi Protected Access WPA & WPA2 Personal and Enterprise/TKIP/AES
LED Indicators	WAN, LAN, WLAN (Link and Activity) Power, Router Disconnect

Advanced Firewall Features	Network Address Translation (NAT) Up to 254 Addresses Stateful Packet Inspection (SPI) AlphaGAP Logical Disconnect (Automatic and Manual) MAC Filtering (Exclusion and Inclusion) Website Filtering Scheduling AlphaGAP Connection Scheduler (ACS) Gaming and Port Control Feature Special Applications and Port Trigger Configurable DMZ Port
Software Features	StreamEngine (R) Technology Router Disconnection Scheduler Up to 256 Firewall Port Configurations Access Control Policies (Parental Control) Internal and External System Logging Static and Dynamic Routing Oversized NAT Table Print Sharing Capability Email Alerts Wireless Distribution Mode (WDS)
Device Management	Internet Explorer v6 or Later, or other Java-enabled Browers and Telnet
Power Requirements	DC Wall Adapter 5.8 Volts 2.4 Amps
Dimentions and Weight	280 x 120 x 40 mm 250 grams
Environmental Operation	32F to 130F (0C to 55C) Humidity 95% Maximum (Non-Condensing)
Mean Time Before Failure (MTBF)	35,000 Hours
Warranty	Limited Life Time Warranty

13. SUPPORT:

13.1 100% Unhackable or Money Back Guarantee:

If the original purchaser can prove that he or she was hacked while using a properly installed AlphaGIGABIT Router, with AlphaGAP Technology enabled, AlphaShield Inc. will accept the return of the product and provide a full refund (with proof of purchase) or replace the product at AlphaShield's option.

13.2 Warranty:

The Manufacturer warrants AlphaGIGABIT Router with an exclusive AlphaShield Limited Lifetime Warranty in workmanship and materials from the date of purchase. The AlphaShield Router will provide years of Network Security and trouble free operation if properly connected and operated as per the instructions in this manual. If you are experiencing any problems with your AlphaGIGABIT Router, please contact technical support at the contact information given below.

Note: Your Alpha Router has no user serviceable component within it. Opening the housing will VOID THE WARRANTY and may even cause permanent damage to the static sensitive electronic devices. For details regarding the AlphaShield Limited Lifetime Warranty, visit . Please note some of the following terms and conditions:

1. If Warranty items are shipped for repair or replacement, AlphaShield is not responsible for lost or damaged packages, please INSURE and obtain a TRACKING number as a safeguard.
2. P.O. Box addresses are NOT accepted for product repair or replacement. You must provide us with a physical address to continue with the warranty Process.
3. AlphaShield's sole liability, and the exclusive remedy, for any acknowledged defect(s) shall be the repair or replacement of the product in question.
4. Customer bears the cost of sending the defective unit(s) to AlphaShield plus any expedited fees, and AlphaShield bears the cost of shipping the replacement unit to customer.
5. AlphaShield does not offer refunds, credits or upgrades.
6. International customers (outside of Canada) are responsible for custom charges including, but not limited to, brokerage, taxes, duties and other fees.
7. Replacements are processed upon product availability.
8. AlphaShield shall NOT be liable under ANY circumstances for any indirect, incidental or consequential damages or lost data.
9. Warranty is available only to the original purchaser.
10. AlphaShield is not responsible for return freight charges resulting from invalid or expired shipments.

.

13.3 Service and Repairs:

In case the AlphaGIGABIT Router device is found to be defective, the Manufacturer will be obligated **only** to replace or repair the defective product provided that the following is determined:

- The product has not been altered or repaired without the written consent of the Manufacturer.
- The product has not failed due to misuse, improper maintenance, carelessness or physical damage.
- No other warranty or condition is implied and the Manufacturer under no circumstances is liable for any damages arising from the use of the AlphaShield Router device.

Please contact the Manufacturer at the following:

Email: tech@alphashield.com

Telephone: 1-866-722-3638

Please note that we cannot accept any returns without a proper RMA (Return Merchandise Authorization) number. An RMA number can be obtained by contacting AlphaShield Inc. prior to the shipment of the unit.

13.4 RMA Card:

AlphaShield Inc. warrants this product to be free of defects and to be fully functional for a period of 24 months from the date of original purchase. AlphaShield will repair or replace at AlphaShield Inc.'s option any unit, without cost, during this period, if the unit is found to be defective for any reason other than abuse or incorrect usage or installation. Do not try to repair the unit. Any modifications of the unit by anyone other than an authorized AlphaShield representative will void the warranty.

If an AlphaShield Router device needs repair, call AlphaShield for a RMA (Return Merchandise Authorization) number and return the defective unit, freight prepaid, along with a brief description of the problem, to the address specified by the Representative. AlphaShield will repair faulty units beyond the warranty program at a nominal charge. Contact an AlphaShield Sales Representative for details and pricing.

RMA # ________________________

Description of problem:

13.5 Copyright:

13.6 Trademark:

AlphaShield, AlphaGAP and the AlphaShield logo are registered trademarks, and/or are registration pending trademarks of AlphaShield Inc. in Canada, United States and other various countries. Other product or company names mentioned herein may be the trade name, trademark, or service mark of their respective owners. The use of any AlphaShield Inc.'s trade names, trademarks or service marks without AlphaShield's express written consent is strictly prohibited.

13.7 Patents:

The accompanying product and software is protected by one or more U.S. and foreign patents and/or patents pending held by AlphaShield Inc.

13.8 Restrictions:

You may not copy, modify, adapt, translate into any language, distribute, or create derivative works based on the software and/or hardware without the prior written consent of AlphaShield Inc. and/or its subsidiaries and certified partners. You may not assign, rent, lease, or lend the software and/or hardware to any person or entity. Any attempt by you to sub-license, transfer, or assign the software and/or hardware will void all warranties and guarantees. You may not decompile, disassemble, reverse engineer, or attempt to reconstruct, identify, or discover any source code, underlying ideas, underlying user interface techniques, or algorithms of the software and/or hardware by any means whatsoever, except to the extent the foregoing restriction is prohibited by applicable law.

13.9 Liability Limitations:

AlphaShield Inc., its agents, employees, suppliers, dealers, and other authorized representatives shall not be responsible or liable, with respect to the product or any other subject matter related thereto, for any special, indirect, punitive, incidental, or consequential damages including, but not limited to, loss of information, business, profits, revenues, goodwill, use, data or other intangible losses (even if such parties were advised of, knew of or should have known of the possibility of such damages), resulting from the use of or the inability to use, the product and its software, under any contract, negligence, strict liability or other theory.

13.10 Customer Remedies:

Any liability of AlphaShield Inc., with respect to software or hardware or the performance thereof or defects therein, under any warranty, negligence, strict liability or other theory, will be limited exclusively to product replacement or, if replacement is inadequate as a remedy or, in AlphaShield Inc.'s opinion, impractical, to refund of the purchase price and termination of the license. An AlphaGIGABIT device that is returned must be accompanied by a copy of the original purchase receipt and a proper RMA (Return Merchandise Authorization) number. This Limited Warranty is void if failure of the AlphaGIGABIT device has resulted from accident, abuse or misapplication. Any replacement AlphaShield will be warranted for the remainder of the original warranty period.

13.11 Notice of Change to Terms and Conditions:

All content, including terms and conditions, contained herein is subject to change without notice. AlphaShield Inc. reserves the right to change or modify the terms and conditions applicable to the use of its products and softwares at any time. Such changes, modifications, additions, or deletions to the terms and conditions of use shall be effective immediately upon notice thereof, which may be given by any means including, but not limited to, posting new terms and conditions on the company's website: www.alphashield.com. Any use of the products and softwares after such change or modification shall be deemed to constitute acceptance by you of such changes, modifications, additions, or deletions.

AlphaShield Inc. may terminate, change, suspend or discontinue any aspect of the terms and conditions, including, but not limited to, the availability of any features on the company's website or the usage of any services currently and/or previously provided by the company, at any time. AlphaShield Inc. may also impose limits on certain features and services or restrict your access to parts of the company's website without notice or liability.

13.12 Replaceable Components and Returns:

The only replaceable part of your AlphaGIGABIT Router is the power adapter. Should you misplace, break or damage your power adapter it can be replaced with a standard 7.5 VDC wall power adapter. The ratings should be 7.5 VDC between 2.75Amp to 3.0Amp center positive. This power adapter can be purchased from various electronic stores and distributors. Should you require a new power adapter, the following 7.5 VDC 2.75Amp can be purchased from RadioShack. The Adapter plug size must be 3.4 mm DE x 1.5 mm DI x 7mm Length.

The AlphaGIGABIT Router requires a positive polarity to be provided to the center conductor of the power plug. Ensure that the proper adapter plug used is connected to provide proper power to the AlphaGIGABIT Router device.

You can also obtain a replacement universal power adapter directly from AlphaShield Inc. AlphaShield Inc. will charge an amount of $8.99 U.S. funds for a replacement power adapter plus any additional shipping and handling charges incurred.

Do not use any other type of power adapter, other than the one specified here within the manual, to provide power to the AlphaGIGABIT Router device. Failure to do so may cause permanent damage to the AlphaGIGABIT Router device and will void the warranty.

14. IMPORTANT NOTICES:

14.1 FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased, please contact the AlphaShield head office.

14.2 FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

14.3 FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

14.4 IC Statement:

Operation is subject to the following two conditions:

1) This device may not cause interference and;

2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 7dBi. An antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 Ohms.

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Heath Canada's website www.hc-sc.gc.ca/rpb.

14.5 IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.